GeBro-BACKUP

Die Online-Datensicherung.

GeBro-BACKUP *v6* User's Guide

In the following document, the GeBro-BACKUP software is named as

- Online Backup Manager software, or
- OBM

29 February 2012

AGENTUR BROGLIE
Moserstr. 13
72760 Reutlingen
www.gebro-backup.de
info@agentur-broglie.de

Online Backup Manager

User's Guide

Copyright Notice

The use and copying of this product is subject to a license agreement. Any other use is prohibited. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without prior written consent.

Information in this manual is subject to change without notice and does not represent a commitment on the part of the vendor. The vendor does not warrant that this document is error free. If you find any errors in this document, please report to the vendor in writing.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Trademarks

Microsoft, Windows, Microsoft Exchange Server and Microsoft SQL Server are registered trademarks of Microsoft Corporation.

Sun, Solaris, SPARC, JAVA and Java Runtime Environment are registered trademarks of Sun Microsystems Inc.

Oracle, Oracle 8i, Oracle 9i, Oracle 10g, Oracle 11g are registered trademarks of Oracle Corporation.

Lotus, Domino, Notes are registered trademark of IBM Corporation.

Red Hat is registered trademark of Linus Toryalds.

Apple and Mac OS X are registered trademarks of Apple Computer, Inc.

All other product names are registered trademarks of their respective owners.

Table of Contents

3.1.1 Installing OBM (Installation wizard) 10
3.1.2 Installing OBM (Command line) 10
3.1.3 Installing OBM (Command line - Silent installation) 11
3.1.4 Configuring OBM 12
3.3.1 Installing OBM on Linux 15
3.3.2 Installing OBM on Solaris 16
3.3.3 Installing OBM on FreeBSD 18
4.1.1 Uninstalling OBM (Control Panel) 24
4.1.2 Uninstalling OBM (Command line) 25
6.1.1 New Backup Set Wizard 42
6.1.2 General 44
6.1.3 Backup Source 45
6.1.4 Backup Schedule 47
6.1.5 Encryption 50
6.1.6 Continuous Data Protection (CDP) 56
6.1.7 In-File Delta 61
6.1.8 Retention Policy 61
6.1.9 Backup Filter 65
6.1.10 Command Line Tool 68
6.1.11 Extra Backup 71
6.1.1.11 Enable off-line backup 72
6.1.2.11 Enable System Logout Backup Reminder 73
6.1.12 Local Copy 74
6.1.13 Options 78
6.1.1.13 Temporary Directory for storing backup files 78
6.1.2.13 Follow Link 79
6.1.3.13 Enable Volume Shadow Copy 81
6.1.4.13 Compression 83
6.1.5.13 Transfer Block Size 84
6.1.6.13 Backup File Permission 85
8.1.1 Restore Menu 94
8.1.1.1 Filter 95
8.1.2.1 Search 97
8.1.3.1 Delete extra files 98
8.1.4.1 Follow Link 100
8.1.5.1 Resolve Link 101
8.1.6.1 Delete backed up directories and files on backup server 102
8.2.1 Restore using the OBM user interface 103
8.2.2 Restore using the web interface 107
8.2.3 Restore using Decrypt File Wizard 110
9.1.1 Block Size 119
9.1.2 Apply to files (Minimum Size) 119
9.1.3 Delta Merging (Enable delta merging) 119
9.1.1.3 Overview 120
9.1.2.3 Limitation 120
9.1.3.3 Delta merge policy 121
9.1.4.3 Delta merging process 121
9.1.5.3 Delta merging example 121

9.1.4 In-File Delta Type 126
9.1.1.4 Advance In-file Delta Type 126
9.1.5 Upload full file when 128
9.1.1.5 No. of Delta 128
9.1.2.5 Delta Ratio 129
10.4.1 For Windows XP, 2003 / R2 132
10.4.2 For Windows Server 2008 / R2, SBS 2011 133
10.5.1 For Windows XP, 2003 / R2 136
10.5.2 For Windows 2008 / R2, SBS 2011 140
10.5.3 For Windows 2008 / R2 Domain Controller 143
11.5.1 Recover volumes with the Recovery Wizard 152
11.5.2 Recover the operating system with the Install Windows Wizard 155
11.5.3 Recover volumes with command 158
11.5.4 Recover with the Windows Recovery Environment 159
13.1.1 Supported versions 175
13.1.2 Requirements and recommendations 175
13.1.3 Limitations 177
13.1.4 Overview 178
13.1.5 How to backup virtual machines on VMware ESXi / ESX Server 179
13.1.6 How to restore virtual machines on VMware ESXi / ESX Server 183
13.1.1.6 How to restore virtual machines to the original hypervisor 183
13.1.2.6 How to restore virtual machines to another hypervisor 191
13.1.7 How to restore individual virtual disk 197
13.1.1.7 How to restore individual virtual disk to the original VM 198
13.1.2.7 How to restore individual virtual disk to a different VM 198
13.2.1 Supported versions 204
13.2.2 Requirements and recommendations 204
13.2.3 Limitations 205
13.2.4 Overview 205
13.2.5 How to backup virtual machines on VMware Server 206
13.2.6 How to restore virtual machines on VMware Server 210
13.2.1.6 How to restore virtual machines to the original hypervisor 210
13.2.2.6 How to restore virtual machines to another hypervisor 218
13.2.7 How to restore individual virtual disk 226
13.2.1.7 How to restore individual virtual disk to the original VM 226
13.2.2.7 How to restore individual virtual disk to a different VM 227
13.3.1 Supported versions 233
13.3.2 Requirements and recommendations 233
13.3.3 Limitations 234
13.3.4 Overview 234
13.3.5 How to backup virtual machines on VMware Fusion 234
13.3.6 How to restore virtual machines on VMware Fusion 239
13.3.1.6 How to restore virtual machines to the original hypervisor 239
13.3.2.6 How to restore virtual machines to another hypervisor 247
13.3.7 How to restore individual virtual disk 255
13.3.1.7 How to restore individual virtual disk to the original VM 255
13.3.2.7 How to restore individual virtual disk to a different VM 255
13.4.1 Supported versions 259
13.4.2 Backup and restore of virtual machines on VMware Player and Workstation 259

14.1.1 Requirements and recommendations 261
14.1.2 Limitations 261
14.1.3 Overview 262
14.1.4 How to backup Microsoft virtual machines 263
14.1.5 How to restore Microsoft virtual machines 267
14.1.6 How to restore individual virtual disk 277
14.1.1.6 How to restore individual virtual disk to original VM 277
14.1.2.6 How to restore individual virtual disk to a different VM 280
14.2.1 Requirements and recommendations 286
14.2.2 Limitations 286
14.2.3 License requirement to backup all virtual machines in a cluster 291
14.2.4 Overview 293
14.2.5 How to backup Microsoft virtual machines in cluster environment 294
14.2.6 How to restore Microsoft virtual machines in cluster environment 298
14.2.7 How to restore individual virtual disk of Microsoft virtual machines in cluster environment 308
14.2.1.7 How to restore individual virtual disk to the original VM 308
14.2.2.7 How to restore individual virtual disk to a different VM 311
15.2.1 Requirements and recommendations 318
15.2.2 Overview 318
15.2.3 How to backup Microsoft Exchange Server 2003 / 2007 319
15.4.1 Requirements and recommendations 330
15.4.2 Overview 330
15.4.3 How to backup Microsoft Exchange Server 2010 331
18.5.1 Restore Microsoft SQL Server 2000 database 400
18.5.1.1 Restore master database 400
18.5.2.1 Restore other system or user database (complete backup) 402
18.5.3.1 Restore other system or user database (differential / transaction log backup) 406
18.5.2 Restore Microsoft SQL Server 2005 / 2008 database 408
18.5.1.2 Restore master database 408
18.5.2.2 Restore other system or user database (complete backup) 410
18.5.3.2 Restore other system or user database (differential / transaction log backup) 414

1 Overview

1.1 Conventions

Convention	Descriptions	Example
Bold	**Important information**	Important: The encrypting key is independent from a backup account's password.
Italic	**Folder path or file path**	***C:\Program Files\OBM***
[]	**Graphical Interface Elements**	**[Backup]**
%%	**File path in Windows format**	**%OBM_HOME%**
$	**File path in Mac OS X format**	**$OBM_HOME**
Italic	**Command**	*sudo ./uninstall.sh*

1.2 Definitions, acronyms and abbreviations

Term/Abbreviation	Definition
OBM	**Online Backup Manager**
OBS	**Offsite Backup Server**
OBM_HOME	**The install location of OBM:** **Windows** ***C:\Program Files\OBM*** **Mac OS X** ***/Applications/OBM***
USERPROFILE	**The location where the operating system stores the user account information.** **Windows XP/2003** ***C:\Documents and Settings*** **Windows Vista/2008/7** ***C:\Users*** **Mac OS X** ***~/.obm***

1.3 System requirements

Minimum	Recommended
OS: Windows XP Mac OS X v10.5 Red hat 4 CentOS 4 Solaris 10 FreeBSD 7.3	OS: Or higher
CPU: n/a	CPU: Multithread supported
Memory: 512 MB	Memory: 1GB or above
Network: TCP/IP	Network: TCP/IP
Java: 1.5u22 *	Java: 1.6u23 *

* Java is included in the software.

1.4 Important notes

Images, workflow or description in this document may be different from your installation. If you are uncertain about any of the instructions provided, please contact your service provider for advices.

2 Best practices and recommendations

This chapter describes the best practices for your backup client application.

2.1 Recommended hardware specification

OBM is recommended to be installed on a 64 bit machine, with multiple CPUs and cores, especially for environment setup with application specific backup module such as virtual machine, MS Exchange, or bare metal backup.

When installing the backup client application, please thoroughly evaluate the computer's specification before the installation to ensure it meets the minimum hardware requirements and recommendations.

For existing users, the backup process may take up a higher amount of CPU and may slow down the client computer due to the multi-thread implementation since version 6. Please consider upgrading your existing client computer to cope with the higher specification demand.

Please refer to chapter 1.3 for the system requirements of OBM.

2.2 JVM (Java Virtual Machine) memory allocation

For resource intensive backup modules such the following:

- MS Exchange Server backup
- MS VM backup
- MS Windows System backup
- ShadowProtect System backup
- System State backup
- VMware VM backup

If you are experiencing performance issues with the backup application, a common cause is insufficient JVM (Java Virtual Machine) memory allocated for the backup application. The default setting of the maximum heap size is 768 MB.

Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation.

Note:
The maximum memory allocated should not exceed 70% of the total memory available for the system.

You can increase the maximum heap size of the application by changing the Xmx values in config.ini, RunOBC.bat, RunOBC32.bat and RunBackupSet.bat

2.3 Storage size for user folder of your operating system

Your backup user profile folder (*.obm*) is stored under the operating system user profile location *${UserProfile}*.

This folder is used for various purposes, such as storage of your backup logs, user configuration files, temporary delta file and other files of temporary nature.

Ensure that sufficient disk space is present on the partition which contains the backup user profile.

2.4 Temporary directory for OBM

For database or application backup modules such as the following:

- MS Exchange Server backup
- MS Windows System backup
- ShadowProtect System backup
- System State backup

Corresponding data are spooled to a temporary directory before they are compressed, encrypted and uploaded onto the backup server.

It is highly recommended that the temporary directory or volume used for these modules is not a system volume (e.g. not the same partition which the operating system is installed on).

It is also recommended that the temporary directory or volume configured to have at least storage space of 150% of the expected backup size.

Regular checks on the temporary directory, for left over files due to previous unsuccessful backup are also recommended.

2.5 Encryption

The encryption key is very important that it is recommended to write down, and make additional copies of the key.

Please store the key in safe location so that it is readily available when needed to restore data.

In some cases, encryption key is administrated by your service provider. Please consult your service provider for further details.

For maximum security, please select an encryption key with more than 8 characters, containing at least two of the following three character groups:

- English uppercase characters (A through Z)

- English lowercase characters (a through z)
- Numerals (0 through 9)

If you lose the encryption key, the data is irretrievable.

2.6 Backup schedule

In general, it is recommended that a daily backup be performed for a server or desktop. For mission critical server, a backup schedule should be configured according to the requirement of your recovery plan.

For computer with multiple backup sets configured, please configure their schedule to different time period to evenly balance the loads of the backup operation on the computer.

2.7 Differential and incremental In-file delta backup

Consider your restore requirements before setting up your In-file delta settings:

A full backup backs up all files in full, providing the fastest restore time as the restore would only require one set of data. But it is the most time-consuming, storage space-intensive and the least flexible of all three types.

A differential In-file delta backup backs up only modified parts of a file since the last full back. Differential In-file delta backup is quicker than full backup because less data are being backed up, but the amount of data being backed up grows with each differential In-file delta backup until the next full backup is performed.

An incremental In-file delta backup also backs up modified parts of a file. The difference is it only backs up the changes that occurred since the last backup, be it full, differential or incremental backup. The result is a smaller and faster backup.

While incremental backups give much greater flexibility, data backed up by long chain of incremental In-file delta backup will take a lot longer to restore, and is prone to data lost (e.g. broken delta chain).

The following table summarizes the benefits and drawbacks of the 3 backup types:

Type	Benefits	Drawbacks
Full	Restoration is the fastest of all three types.	Backup process is the slowest of all three types. Highest storage requirement.

Differential	Backup speed is faster than full backup. Restoration is faster than data backup with incremental In-file delta. Less storage space is need than a full backup.	Restoration is slower than data backup with full backup. Backup process is slower than incremental In-file delta backup.
Incremental	Backup process is fastest of all three types. Least storage space is required.	Restoration is the slowest of all three types. Prone to data lost.

Assuming that a daily backup job is performed, the following In-file delta setting is recommended for your backup operation:

Weekday	**Backup Type**
Day 1	Full
Day 2	Incremental
Day 3	Incremental
Day 4	Incremental
Day 5	Differential
Day 6	Incremental
Day 7	Incremental

2.8 Difference between Local Copy and Seed Load

The Local Copy and Seed Load features are very similar in terms of what they do.

While the Local Copy feature is designed for user who wants to an extra copy of the backup data locally, at the client site, the Seed Load feature is designed for initial backup of large data (e.g. initial backup of large MS Exchange database).

A Seed Load backup is performed onto a removable storage device to be imported on the backup server physically, bypassing the bottleneck of Internet backup.

The major differences between Local Copy and Seed Load are:

Feature	**Local Copy**	**Seed Load**
Retention Policy	Retention policy can be applied on local copy backup.	No retention policy is applied on seed load backup.

In-file Delta	Advance In-file Delta type setting can be applied on local copy backup.	No In-file Delta type setting is applied on seed load backup.
Backup Schedule	Local copy backup can be performed manually or by schedule.	Seed load backup can only be performed manually.

For performance consideration, it is highly recommended that the local copy backup be performed on a local hard disk, and not to a network location.

2.9 Recommended backup exclusions

Backing up system, system cache, redundant or non-essential files, such as Windows page file can cause unnecessarily high data change rates and excessive use of network bandwidth, affecting backup operations negatively.

Consider excluding the following files when configuring your backup source location.

Operating system	Directory path
Windows	C:\hiberfil.sys C:\Pagefile.sys C:\Program Files* C:\RECYCLER C:\System Volume Information C:\Windows* ${App_Data}\Avg7 ${App_Data}\Avg8 ${App_Data}\Kaspersky Lab ${App_Data}\McAfee ${App_Data}\McAfee.com ${App_Data}\Microsoft ${App_Data}\Sophos ${App_Data}\Symantec **.tmp *\Application Data\Macromedia* *\Application Data\Mozilla* *\Local Settings\Application Data\Microsoft* *\ntuser.dat
Linux	/dev /lost+found /proc /sys /tmp /var/empty /var/lock

	/var/run /var/spool /var/tmp

2.10 Disable SELinux (Security-Enhanced Linux)

For backup client installation on Linux, it is recommended to disable the SELinux (Security-Enhanced Linux) feature to avoid error during your backup operation.

2.11 Single backup user account for multiple computers

For backup of multiple computers with a single account, separate backup set for each computer must be created, because backup set cannot be shared for multiple computers.

For administrative concerns and considerations (e.g. data lost due to incorrect configuration), it is not recommended that a backup user account to have more than 10 backup sets for backup of multiple computers.

Incorrect configuration can lead to data lost.

2.12 Power options - plan settings consideration

Windows' power options are configured to put a computer to low power mode (sleep or hibernate mode) automatically after a user specified time of inactivity (no usage of mouse or keyboard).

- If a computer is in low power mode when a scheduled backup should execute, OBM will not start up the computer to execute the backup.

  When the computer moves out of the low power state, OBM will not execute the missed backup job. This can lead to missed backup.

- If a backup job is running when the computer enters low power state, OBM cannot prevent the computer from going into hibernation.

To prevent the above events, consider disabling or changing the client machine's power options to allow scheduled backup to be triggered, and to allow the backup job to be completed.

2.13 Consideration when using Continuous Data Protection (CDP)

Some advantages of using CDP include:

- CDP prevents loss of data as the modified contents of the files are backed up automatically in close to real-time.
- Frequently modified data is backed up in almost real-time. Thus, you can accurately restore an earlier version created on the same day.

Although CDP can be a helpful feature, the protection offered by CDP is often heralded without consideration of the disadvantages that it can present.

Specifically, the continuous CPU, memory and bandwidth usage can adversely affect the corresponding machine's performance.

Please consider the limitations imposed by CDP before utilizing such feature.

CDP is not a replacement for traditional schedule backup, but is a complimentary backup, which works along with the scheduled backup to provide timely protection for your data.

2.14 Size of your backup source

The total number of files selected as backup source and the relative size of each file impacts backup performance. Fastest backups occur when the source contains fewer large size files, while slowest backups occur when the source contains millions of small files.

For backup set with huge amount of files, please consider splitting the set into multiple sets with smaller source to improve the speed of the backup operation.

2.15 Recovery plan and routine recovery test

Consider performing routine recovery test to ensure your backup is setup and performed properly. Performing recovery test can also help identify potential issues or gaps in your recovery plan.

For best result, it is recommended that you keep the test as close as possible to a real situation. Often times when a recovery test is to take place, administrators will plan for the test (e.g. reconfigure the test environments, restoring certain data in advance). For real recovery situation, administrator will not get a chance to do that.

It's important that user does not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless. There might be flaws identified in the plan throughout the test and it is important to identify those flaws.

3 Installing OBM

This chapter describes how to install the backup client application.

3.1 Installing OBM on Windows platforms

There are three installation methods available:

- Installation wizard
- Command line
- Command line (Silent installation)

3.1.1 Installing OBM (Installation wizard)

1. Download the OBM installer (obm-win.exe) from the vendor.
2. Follow the instructions provided by Installation Wizard to complete the installation.
3. When completed, a system tray icon for OBM will be installed, and OBM will be launched automatically.

3.1.2 Installing OBM (Command line)

This method is especially useful for installation on Windows Server 2008 Core.

1. Download the OBM installer from OBS.

```
>wget http://obm-download-link/obm-win.exe
```

2. Execute the installation file with the appropriate switches:

```
>obm-win.exe /LANG=en /TASKS="Everyone"
```

Syntax:
obm-win.exe [{/LANG=xx}] [{/TASK="option"}]

Parameter	Description
/LANG=xx	**Install the backup application in the language Selected.**

/TASK="option"	**Install the backup application available to all users or one user only (e.g. me only).**

Value	Description
xx	**Abbreviations of the language to install the backup application in (e.g. en, it, fr).**
option	**Everyone or MeOnly.**

3. Press Enter.

3.1.3 Installing OBM (Command line - Silent installation)

1. Open a Windows command prompt (with an administrative user account on the machine).
2. Download the OBM installer from the OBS.

```
>wget http://obm-download-link/obm-win.exe
```

3. Execute the installation file with the appropriate switches:

```
>obm-win.exe /VERYSILENT /LANG=en /TASKS="Everyone"
```

Syntax:
obm-win.exe [{/SILENT | /VERYSILENT}] [{/LANG=xx}] [{/TASK="option"}]

Parameter	Description
/SILENT	**Install the backup application showing the installation process.**
/VERYSILENT	**Install the backup application hiding the installation process.**
/LANG=xx	**Install the backup application in the language Selected.**
/TASK="option"	**Install the backup application available to all users or one user only (e.g. me only).**

Value	Description

xx	**Abbreviations of the language to install the backup application in (e.g. en, it, fr).**
option	**Everyone or MeOnly.**

4. Press Enter.

3.1.4 Configuring OBM

1. Launch the OBM user interface by double clicking on the desktop icon.
2. Enter the backup server hostname in the [Backup Server] field.
3. *Optional* - For machine that requires Internet connection through proxy, select the [Use proxy to access the backup server] option, and fill in the settings within the [Proxy setting] section.
4. Press the [Next] button afterward.
5. *Optional* - If you do not have a backup user account, you can register for a trial user account with the following steps:
   - Enter the [Login Name] and [Password] of your choice.
   - Enter your [Email] address in the textbox provided.
   - Press the [Submit] button.
6. If you already have a backup user account, select [Already a user?] and logon to the server with your existing login credentials.
7. For first time login, you will be guided to create a backup set:
   - Select the [Backup Source] for the backup set.
   - Configure a backup schedule for unattended backups.
   - For backup set with backup schedule and network shared drive selected as backup source, the [User Authentication for Windows] is a **mandatory field**.
   - Select an encryption setting for your backup set.
   - Accept the default encryption settings (using the backup user account's password string as encrypting key) if no change are necessary.

     Important:
     Even with the default encryption setting selected, the encryption key is independent from a backup account's password.

Encryption settings are set at a backup set's creation time, even if the password is changed afterward, the encryption key remain the same.

It is **very important** that the encryption key is written down, and additional copies of the key are made, and stored in safe places so that it is readily available when needed to restore data.

If the encryption key is lost, the data is irretrievable.

- Press the [OK] button to complete the configuration of backup set.
- Scheduled backup will run automatically at the configured schedule time.

8. Click [Backup] button on the left panel to perform a backup immediately.
9. Setup is now completed.

3.2 Installing OBM on Mac OS X platforms

1. Download the OBM installer from the website.
2. Expand the archive and execute the OBM package.
3. Follow the instructions provided by Installation Wizard to complete the installation.
4. Launch the OBM user interface by double-clicking on the desktop icon.
5. Enter the backup server hostname in the [Backup Server] field.
6. *Optional* - For machine that requires Internet connection through proxy, select the [Use proxy to access the backup server] option, and fill in the settings within the [Proxy setting] section
7. Press [Next] afterward.
8. *Optional* - If you do not have an backup user account, you can register for a trial user account with the following steps:
   - Enter the [Login Name] and [Password] of your choice.

     Note:
     Minimum length of the password is 6 characters.
   - Enter your [Email] address in the textbox provided.
   - Press the [Submit] button.
9. If you have a backup user account already, select [Already a user?] and logon to the server with your existing login credentials.
10. For first time login, you will be guided to create a backup set:
    - Enter a backup set name and select the backup module type.
    - Assuming that is a file backup set; select the [Backup Source] for the backup set.
    - Configure a backup schedule for unattended backups.
    - Select an encryption setting for your backup set.
    - Accept the default encryption settings (using the backup user account's password string as encrypting key) if no change is necessary.

      Important:
      Even with the default encryption setting selected, the encryption key is independent from a backup account's password.

Encryption settings are set at a backup set's creation time, even if the password is changed afterward, the encryption key remain the same.

It is **very important** that the encryption key is written down, and additional copies of the key are made, and stored in safe places so that it is readily available when needed to restore data.

If the encryption key is lost, the data is irretrievable.

- Press the [OK] button to complete the configuration of backup set.
- Scheduled backup will run automatically at the configured schedule time.

11. Click [Backup] button on the left panel to perform a backup immediately.
12. Setup is now completed.

*For further details of each step, please refer to the following chapters.

3.3 Installing OBM on Linux / FreeBSD / Solaris

3.3.1 Installing OBM on Linux

1. Download the OBM tarball release from the vendor website.
2. Logon as root user in the Linux machine.
3. Create a new $OBM_HOME directory (e.g. /usr/local/obm):

```
# mkdir -p /usr/local/obm
```

4. Unpack the install package to $OBM_HOME:

```
# cd /usr/local/obm
# gunzip obm-nix.tar.gz
# tar -xf obm-nix.tar
```

5. For custom JRE - Install JRE v1.6 or above, and make note of the JRE installation path (e.g. /usr/java).

   Note:
   Custom JRE is only required for client machine not running on x86 or x64.

   - Create a symbolic link for JRE:

```
# ln –sf /usr/java /usr/local/obm/jvm
```

   - Set the $JAVA_HOME environment variable:

```
# export JAVA_HOME=/usr/java
```

6. Install OBM and its related services by using the following commands:

```
# cd /usr/local/obm
# ./bin/install.sh > install.log
```

   Details of the installation can be found under the install.log file.

3.3.2 Installing OBM on Solaris

1. Download the OBM tarball release from the vendor website.
2. Logon as root user in the Solaris machine.
3. Install the *SUNWgtar* package from the Solaris Installation Media which contain the GNU tar util.
4. Create a new $OBM_HOME directory (e.g. /usr/local/obm):

```
# mkdir –p /usr/local/obm
```

5. Unpack the install package to $OBM_HOME:

```
# cd /usr/local/obm
# gtar –zxf obm-nix.tar.gz
```

6. Remove the bundled Java JRE:

```
# rm –rf /usr/local/obm/jre32
# rm –rf /usr/local/obm/jre64
```

7. Install JRE v1.6 or above, and make note of the JRE installation path (e.g. /usr/java).

8. Create a symbolic link for JRE:

```
# ln –s /usr/java /usr/local/obm/jvm
```

9. Set the $JAVA_HOME environment variable:

```
# JAVA_HOME=/usr/java;export JAVA_HOME
```

10. Install OBM and its related services by using the following commands:

```
# cd /usr/local/obm
# ./bin/install.sh > install.log
```

Details of the installation can be found under the install.log file.

3.3.3 Installing OBM on FreeBSD

Note that the following steps assumed that Diablo JRE 1.6.0 is already installed.

Diablo JRE 1.6.0 can be downloaded from:
http://www.freebsdfoundation.org/downloads/java.shtml

1. Download the OBM tarball release from the vendor website.
2. Logon as root user in the FreeBSD machine.
3. Create a new $OBM_Home directory (e.g. /usr/local/obm):

```
# mkdir -p /usr/local/obm
```

4. Unpack the install package to $OBM_Home:

```
# cd /usr/local/obm
# gunzip obm-nix.tar.gz
# tar -xf obm-nix.tar
```

5. Remove the bundled Java JRE:

```
# rm -rf /usr/local/obm/jre32
# rm -rf /usr/local/obm/jre64
```

6. Create a symbolic link for JRE:

```
# ln -sf "/usr/local/diablo-jre1.6.0" "/usr/local/obm/jvm"
```

If you are using csh shell, you need to type rehash and hit [Enter] for the symbolic link to take effect.

For other shell, please use the following command:

```
# setenv JAVA_HOME "/usr/local/diablo-jre1.6.0"
```

7. Install OBM and its related services by using the following commands:

```
```

```
# cd /usr/local/obm
# ./bin/install.sh > install.log
```

Details of the installation can be found under the install.log file in $OBM_HOME/bin.

8. Enable the backup scheduler and auto upgrade services at machine startup by adding the following entries in the system file */etc/rc.conf*:

```
obmaua_enable="YES"
obmscheduler_enable="YES"
```

Run the following scripts:

```
# /usr/local/etc/rc.d/obmscheduler start &
# /usr/local/etc/rc.d/obmaua start &
```

3.4 Configure OBM via X-Windows

1. Set the DISPLAY environment variables.

   sh, bash:

```
DISPLAY=IP_ADDRESS_OF_XTERMINAL[:0.0]; export DISPLAY
```

   For example:

```
DISPLAY=:0.0; export DISPLAY
or DISPLAY=127.0.0.1; export DISPLAY
or DISPLAY=127.0.0.1:0.0; export DISPLAY
or DISPLAY=192.168.0.2; export DISPLAY
or DISPLAY=192.168.0.2:0.0; export DISPLAY
```

   csh:

```
# setenv DISPLAY IP_ADDRESS_OF_XTERMINAL[:0.0]
```

For example:

```
setenv DISPLAY :0.0
or setenv DISPLAY 127.0.0.1
or setenv DISPLAY 127.0.0.1:0.0
or setenv DISPLAY 192.168.0.2
or setenv DISPLAY 192.168.0.2:0.0
```

2. Launch the OBM user interface.

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

3. Enter the backup server hostname in the [Backup Server] field.

4. *Optional* - For machine that requires Internet connection through proxy, select the [Use proxy to access the backup server] option, and fill in the [Proxy setting] section.

5. Press [Next] afterward.

6. *Optional* - If you do not have an backup user account, you can register for a trial user account with the following steps:

   - Enter the [Login Name] and [Password] of your choice.

     Note:
     Minimum length of the password is 6 characters.

   - Enter your [Email] address in the textbox provided.

   - Press the [Submit] button.

7. If you have a backup user account already, select [Already a user?] and logon to the server with your existing login credentials.

8. For first time login, you will be guided to create a backup set:

   - Select the [Backup Source] for the backup set.

   - Configure a backup schedule for unattended backups.

   - Select an encryption setting for your backup set.

   - Accept the default encryption settings (using the backup user account's password string as encrypting key) if no change is necessary.

Important:

Even with the default encryption setting selected, the encryption key is independent from a backup account's password.

Encryption settings are set at a backup set's creation time, even if the password is changed afterward, the encryption key remain the same.

It is **very important** that the encryption key is written down, and additional copies of the key are made, and stored in safe places so that it is readily available when needed to restore data.

If the encryption key is lost, the data is irretrievable.

- Press the [OK] button to complete the configuration of backup set.
- Scheduled backup will run automatically at the configured schedule time.

9. Click [Backup] button on the left panel to perform a backup immediately.
10. Setup is now completed.

*For further details of each step, please refer to the following chapters.

3.5 Command line mode

1. Backup set cannot be created in command line mode.

   Before accessing the backup application in command line mode, please use the web interface to create the initial backup set:

   - Login to the web interface.
   - To **create** the initial backup set:
     - Select the [Backup Set] tab, and [Add].
     - Select the corresponding backup type, and [Update].
     - Configure the backup set by entering the corresponding information in the available fields, such as backup set name, source, and schedule.
     - Click [Update] when complete.
   - To **modify** an existing backup set.
     - Select the [Backup Set] tab, and the corresponding set from the [Backup Set] drop down menu.
     - Modify the backup set setting as required.
     - Click [Update] when complete.
   - To **remove** an existing backup set:
     - Select the [Backup Set] tab, and the corresponding set from the [Backup Set] drop down menu.
     - Click [Remove]

2. Access the backup application in command line mode with the Backup Configurator:

```
# sh /usr/local/obm/bin/Configurator.sh
```

3. Enter the login credentials, backup server URL, connection protocol, and proxy settings as requested:

```
Login Name: Username
Password: ****************************
Backup Server URL: backup.server.com
Which Protocol? (1)Http (2) Https: 2
Use proxy? (Y)es or (N)o: Y
```

```
Proxy Type? (1)Http/Https Proxy (2) SOCKS: 1
Enter proxy server: proxy.server.com
Enter proxy port: 123
Enter proxy username (optional): username
Enter proxy password (optional): ********************
```

4. Configure the encryption setting and schedule setting (e.g. if the backup set should run on this computer) of the initial or a newly created backup set as requests:

```
Found new backup set 'BackupSetName'
Please enter the following values for this backup set:

Encrypting Algorithm?
(1) Twofish (2) AES (3) Triple DES (4) No Encryption: 2
Encrypting Key: ****************
Re-Enter Encrypting Key: ******************
Encrypting Mode? (1)ECB (2) CBC: 1
Run scheduled backup on this computer? (Y)es or (N)o: Y
```

5. The Backup Configurator can also be used to modify configuration settings of existing backup set:

```
Main Menu:
----------
(1). List Backup Setting
(2). Change Password
(3). Change Network Setting
(4). Change run scheduled backup setting
(5). Toggle Masked Field (Password, Encryption Key)
(6). Generate Configuration Report (text format)
(7). Quit

Your Choice:
```

6. To perform a backup immediately, execute the command below.

```
# sh /usr/local/obm/bin/RunBackupSet.sh [BackupSetName]
```

7. Setup is now completed.

*For further details of each step, please refer to the following chapters.

4 Uninstalling OBM

This chapter describes how to uninstall the backup client application.

4.1 Uninstalling OBM on Windows platforms

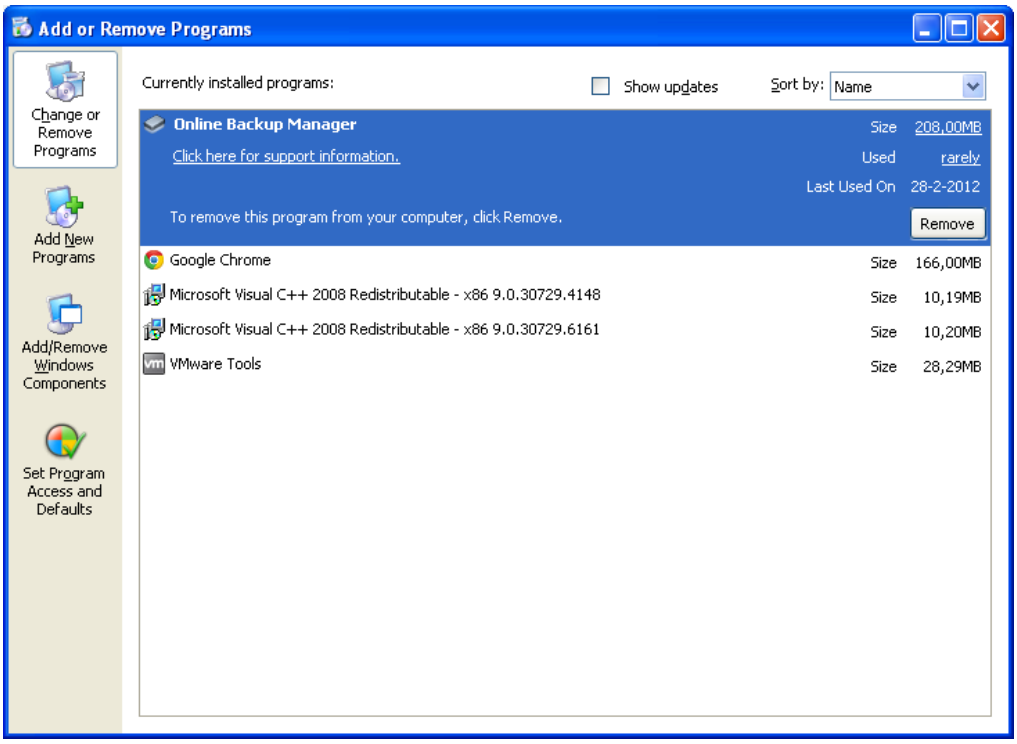
There are two un-installation methods available:

- Add or Remove Programs (Control Panel)
- Command line

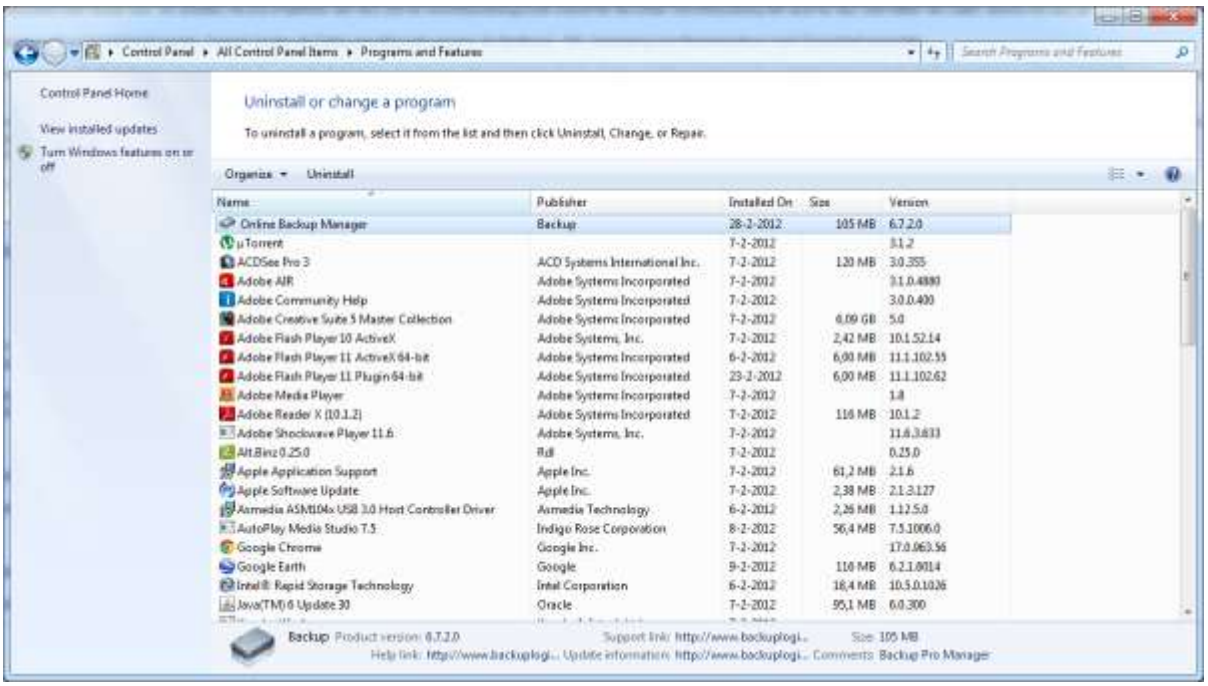
4.1.1 Uninstalling OBM (Control Panel)

1. Open Start menu, select [Control Panel].

- Select [Add or Remove Programs] for Windows XP / 2003



- Select [Programs and Features] for Windows Vista or above



2. Select [Online Backup Manager] from the list and press the [Remove] or [Uninstall] button.

4.1.2 Uninstalling OBM (Command line)

1. Open a Windows command prompt (with an administrative user account on the machine).

2. Uninstall OBM by running the following command:

```
>cd C:\Program Files\OBM
>unins000.exe
```

4.2 Uninstalling OBM on Mac OS X platforms

1. Uninstall OBM by running the following command in terminal:

```
>cd $OBM_HOME/bin
>sudo ./uninstall.sh
```

2. Remove all backup setting files by running the following command in terminal:

```
>rm -rf ~/.obm
```

4.3 Uninstalling OBM for Linux / FreeBSD / Solaris

1. Uninstall the backup application by running the uninstall scripts:

```
# sh /usr/local/obm/bin/uninstall.sh
```

2. Remove all installation files by running the following command:

```
# rm -rf /usr/local/obm
```

3. Remove all backup setting files by running the following command:

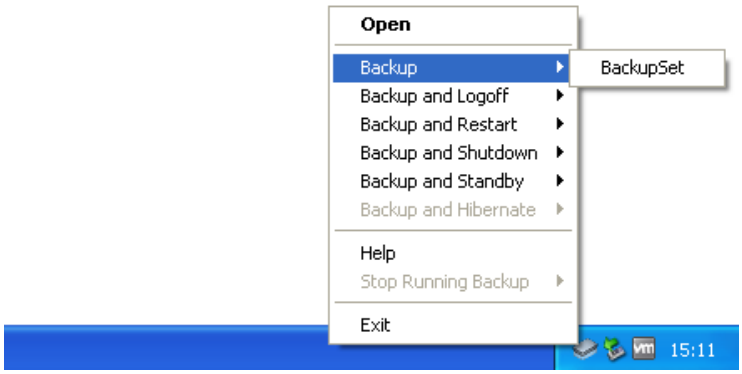
```
# rm -rf ~/.obm
```

5 Getting started with OBM

This chapter describes the various features available in the backup client application.

5.1 System tray launcher (Windows only)

After a successful installation of OBM, a system tray icon will be installed, and displayed under the Windows system tray area.



Right clicking on the OBM system tray icon will display a menu, providing the following functions:

Menu Item	Description
Open	**Click to open the logon dialog.**
Backup	**Click to perform backup for a specific backup set in silent background mode.**
Backup and Logoff	**Click to perform backup for a specific backup set in silent background mode and logoff from Windows when the job is completed.**
Backup and Restart	**Click to perform backup for a specific backup set in silent background mode and restart Windows when the job is completed.**
Backup and Shutdown	**Click to perform backup for a specific backup set in silent background mode and shutdown Windows when the job is completed.**
Backup and Standby	**Click to perform backup for a specific backup set in silent background mode and enter the Standby mode of Windows when the job is completed.**
Backup and Hibernate	**Click to perform backup for a specific backup**

	set in silent background mode and enter the Hibernate mode of Windows when the job is completed
Help	**Open the help dialog.**
Stop running backup	**Click to stop a running backup job chosen from the sub-menu.**
Exit	**Click to closes this system tray launcher application.**

*The availability of options listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

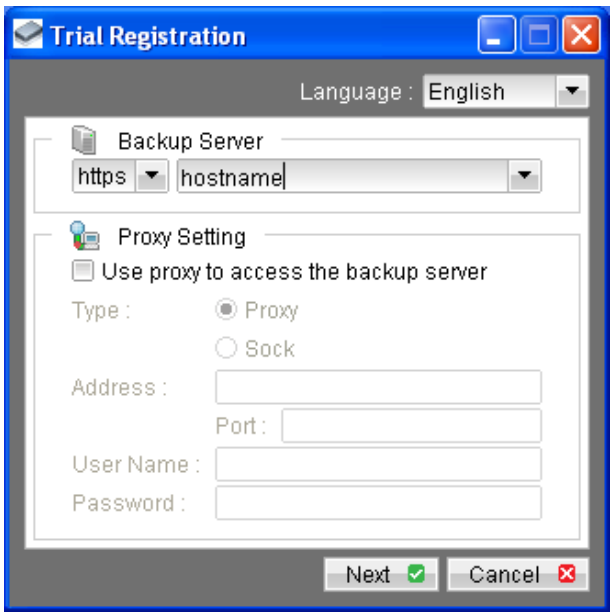
5.2 Logon dialog

For backup client computer on Windows, double-click on the OBM desktop icon or right-click on the system tray icon:

For backup client computer on Linux, enter the following command to start the OBM graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

For initial login, the trial registration dialog will be displayed.

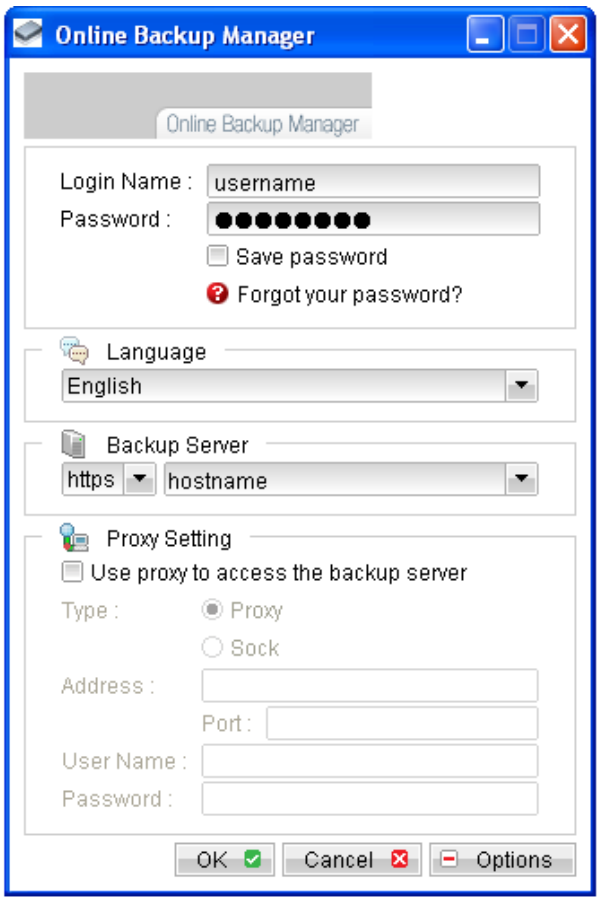


Menu Item	Description
Language	**Drop down menu for selecting language to start the backup application.**

Backup Server	**Input box for entering hostname or IP address of the backup server.**
http / https	**Drop down menu for selecting http or https protocol when connecting to the backup server.**
Proxy Setting	**Input area for entering proxy setting such as address, port, proxy username and password.**
Login Name	**Input box for entering trial backup user login name.**
Password	**Input box for entering trial backup user password.**
Contact	**Input box for entering trail backup user email contact.**
Submit	**Click to create the trial backup user account.**

*The availability of options listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

For sub-sequence login, the login dialog will be displayed.



Menu Item	Description
Login Name	**Input box for entering backup user account login name.**
Password	**Input box for entering backup user account password.**
Save password	**Checkbox to enable or disable password saving.**
Forgot your password?	**Click to request for lost password.**
Options	**Click to access advance option such as [Language], [Backup Server] and [Proxy Setting].**
Language	**Drop down menu for selecting language to start the backup application.**
Backup Server	**Input box for entering hostname or IP address of the backup server.**
http / https	**Drop down menu for selecting protocol when connecting to the backup server.**
Proxy Setting	**Input area for entering proxy setting such as address, port, proxy username and password.**

*The availability of options listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Press the [Option] button to access the [Language], [Backup Server] and [Proxy setting] settings.

Configure the backup server information by entering the server hostname (e.g. backup.server.com) or IP address (e.g. 192.168.1.1) of the backup server in the [Backup Server] field.

For backup server that accepts connection on custom port only, append the hostname or IP address in the [Backup Server] field, by adding a semi-colon (:) and the custom port number at the end.

Example:
backup.server.com:8080 / 192.168.1.1:8443

For security concerns, you can configure the backup client application to communicate with the backup server in SSL protocol (Secure Socket Layer), select [https] from the dropdown menu at the [Backup Server] section.

Enter your login credentials in the [Login Name] and [Password] fields.

If you do not remember your password, press the [Forgot your password?] button to retrieve a forgotten password email.

Please do not attempt to login with an incorrect password, as a backup user account will be locked after 3 bad password attempts. Backup job cannot be run for backup user account with status as locked.

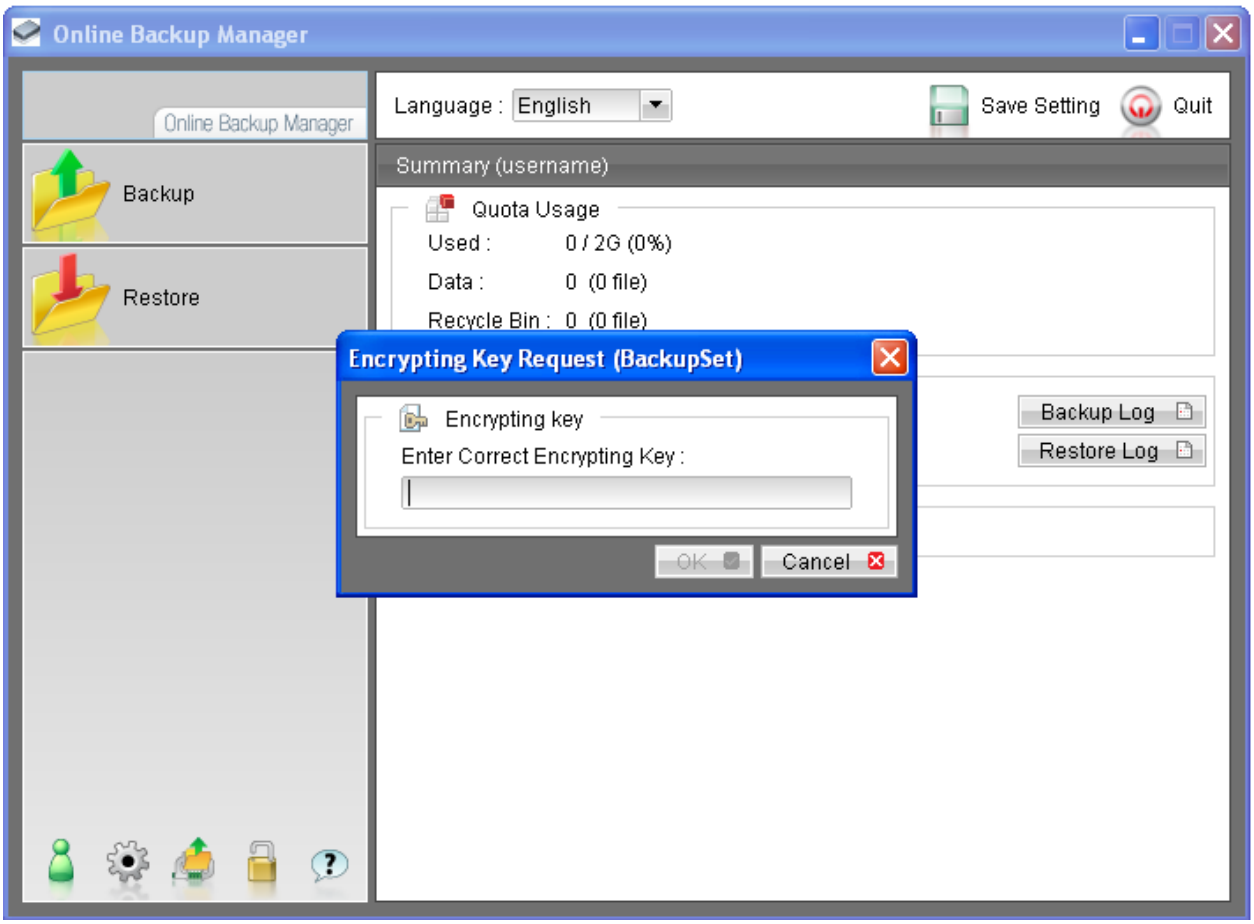
Please contact your service provider to unlock your account if it is locked.

Configure which language to start the backup application in by select the language of your choice under the [Language] drop down menu. For the list of supported languages, please refer to Appendix A.

To enable [Proxy setting], select the [Use proxy to access the backup server] checkbox button, and enter the corresponding proxy information. For [Sock] proxy, both v4 and v5 without user authentication are supported.

Press [OK] to login when all configurations are entered.

For initial login of existing backup user on new computer, you will be prompted for the encrypting key of all existing backup set.



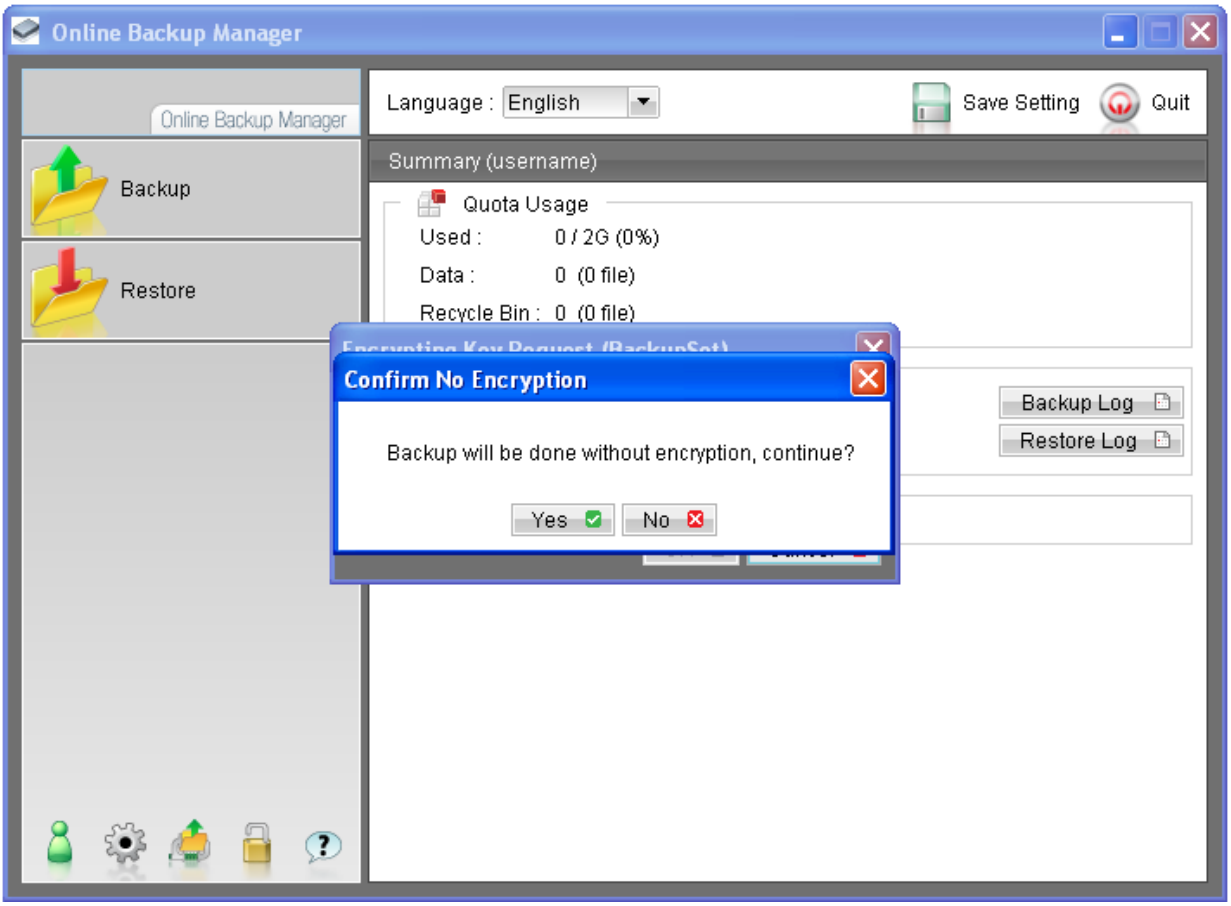
Menu Item	Description

Enter Correct Encrypting Key	**Input box for entering encrypting key of existing backup set.**
OK	**Click to confirm on encrypting key.**
Cancel	**Click to proceed without using encrypting key.**

Enter the correct encrypting key and click [OK] to proceed.

Alternatively, if the encrypting key is lost, press [Cancel] to proceed without encryption (e.g. for all backup job performed afterward).

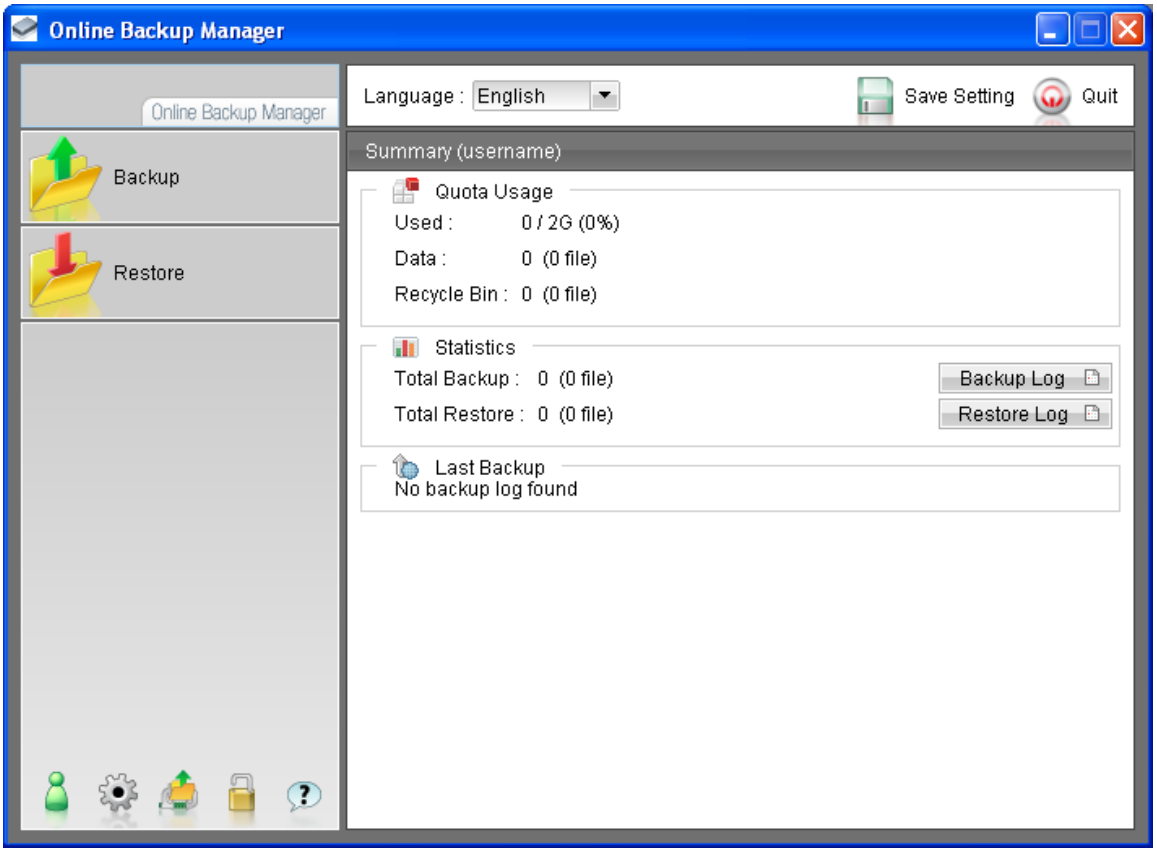
This would allow data backed up in the future to be restore-able (as they are no longer encrypted), but existing data that are already encrypted by the lost encrypting key would not be restore-able.



In case of encrypting key lost, it is strongly recommended that a new backup set be created, to ensure that data backed up in the future is encrypted and restore-able.

5.3 OBM main window

The main window will be displayed after a successful login.



Icon	Menu Item	Description
	Backup	**Click to perform backup for an existing backup set.**
	Restore	**Click to access the restore menu, for restoring backed up data.**
	Save Setting	**Click to save settings.**
	Quit	**Click to exit out of the backup application.**
	User Profile	**Click to access the user profile menu.**

	Backup Setting	**Click to access the backup setting menu.**
	Decrypt Local Copy Wizard	**Click to access the decrypt local copy wizard.**
	Decrypt File Wizard	**Click to access the decrypt file wizard.**
	About A-Click Backup	**Click to access the About A-Click Backup dialog.**
	Language	**Drop down menu for selecting language to be displayed.**
	Backup Log	**Click to view previous backup log.**
	Restore Log	**Click to view previous restore log.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

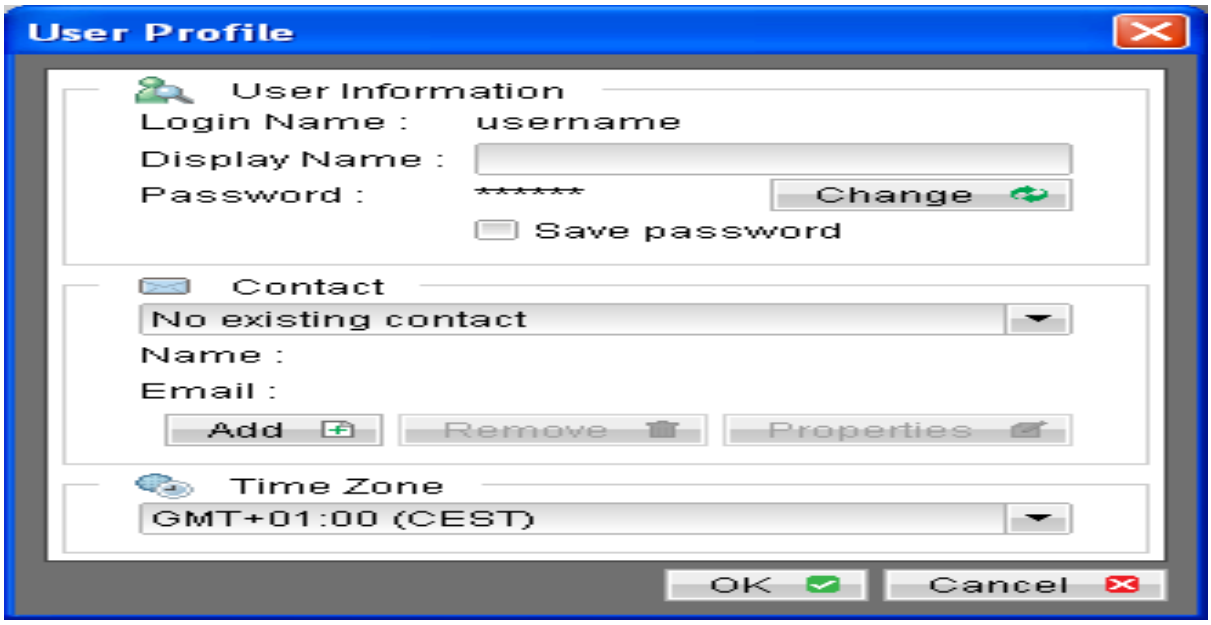
Click on the [Backup] button to perform a backup for an existing backup set.

Click on the [Restore] button to restore backed up data from the backup server to the client machine.

Other options will be discussed in the following chapters.

5.4 User Profile

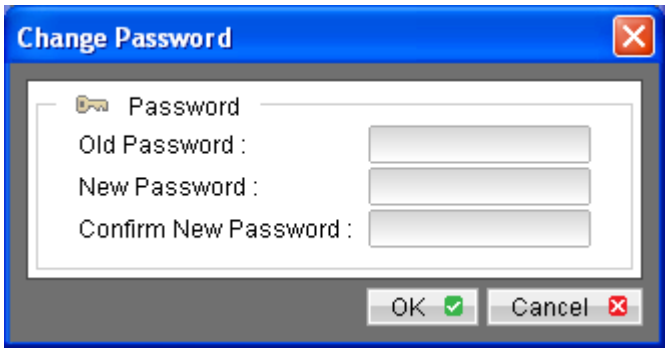
To access the user profile dialog, click on the [User Profile] button at the application's main window.



Menu Item	Description
Display Name	**Input box for entering alias of the backup user account.**
Change	**Click to access the change password dialog.**
Save password	**Checkbox to enable or disable password saving.**
Add	**Click to add contact information.**
Remove	**Click to remove contact information.**
Properties	**Click to edit existing contact information.**
Name	**Input box for entering contact name of the backup user account.**
Email	**Input box for entering contact email address of the backup user account.**
Time Zone	**Dropdown menu for time zone setting.**

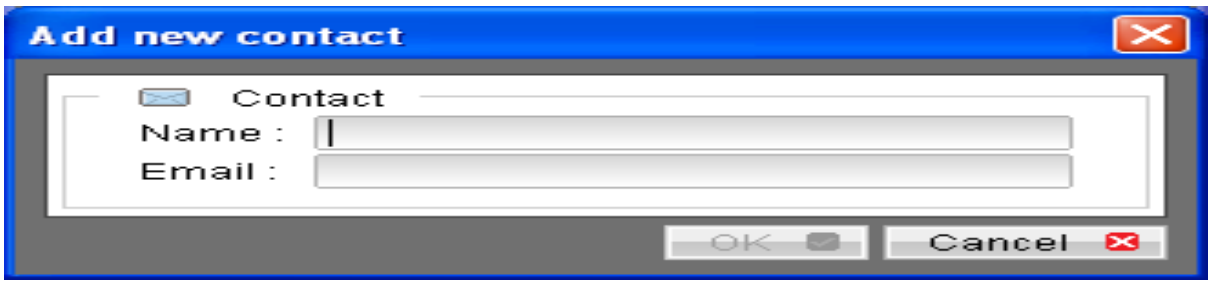
*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

You can change the backup user account's password, by pressing the [Change] button. A change password dialog will be displayed afterward.



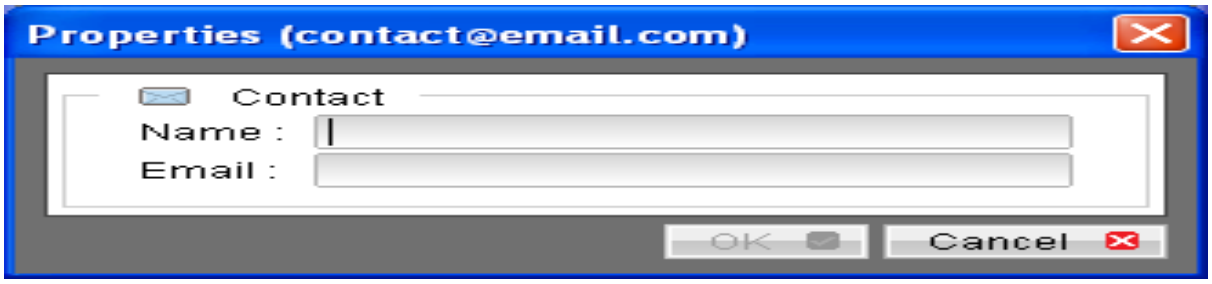
Enter your [Old Password] (e.g. existing password) and [New Password] into the corresponding textbox and press [OK].

To add new contact information for the backup user account, select [Add] to open the [Add new contact] dialog.



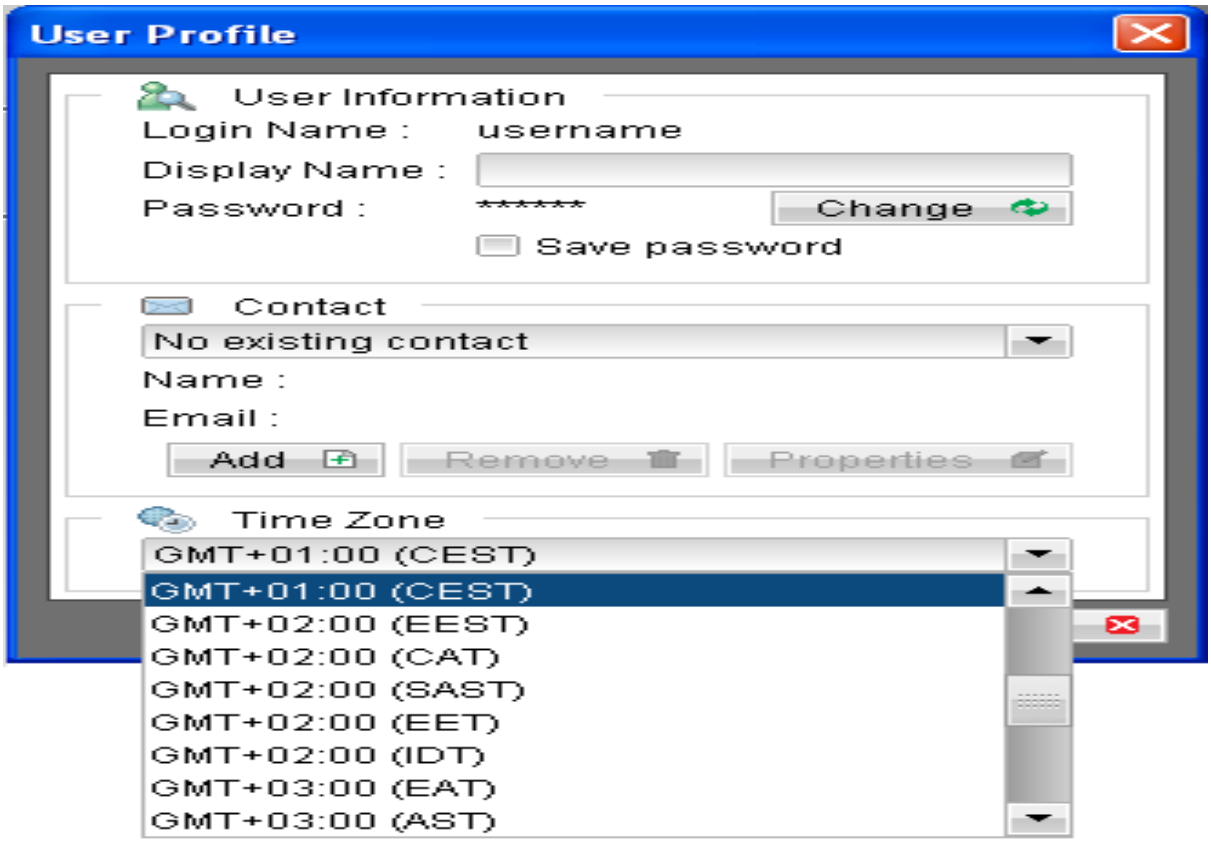
Enter the corresponding information such as [Name] and [Email] in the corresponding field, and press [OK].

To update existing contact of the backup user account, select the corresponding contact from the [Contact] drop down menu, and select [Properties].



To delete existing contact of the backup user account, select the corresponding contact from the [Contact] drop down menu, and select [Remove].

To change the backup user account's time zone setting, select the corresponding time zone from the [Time Zone] drop down menu.

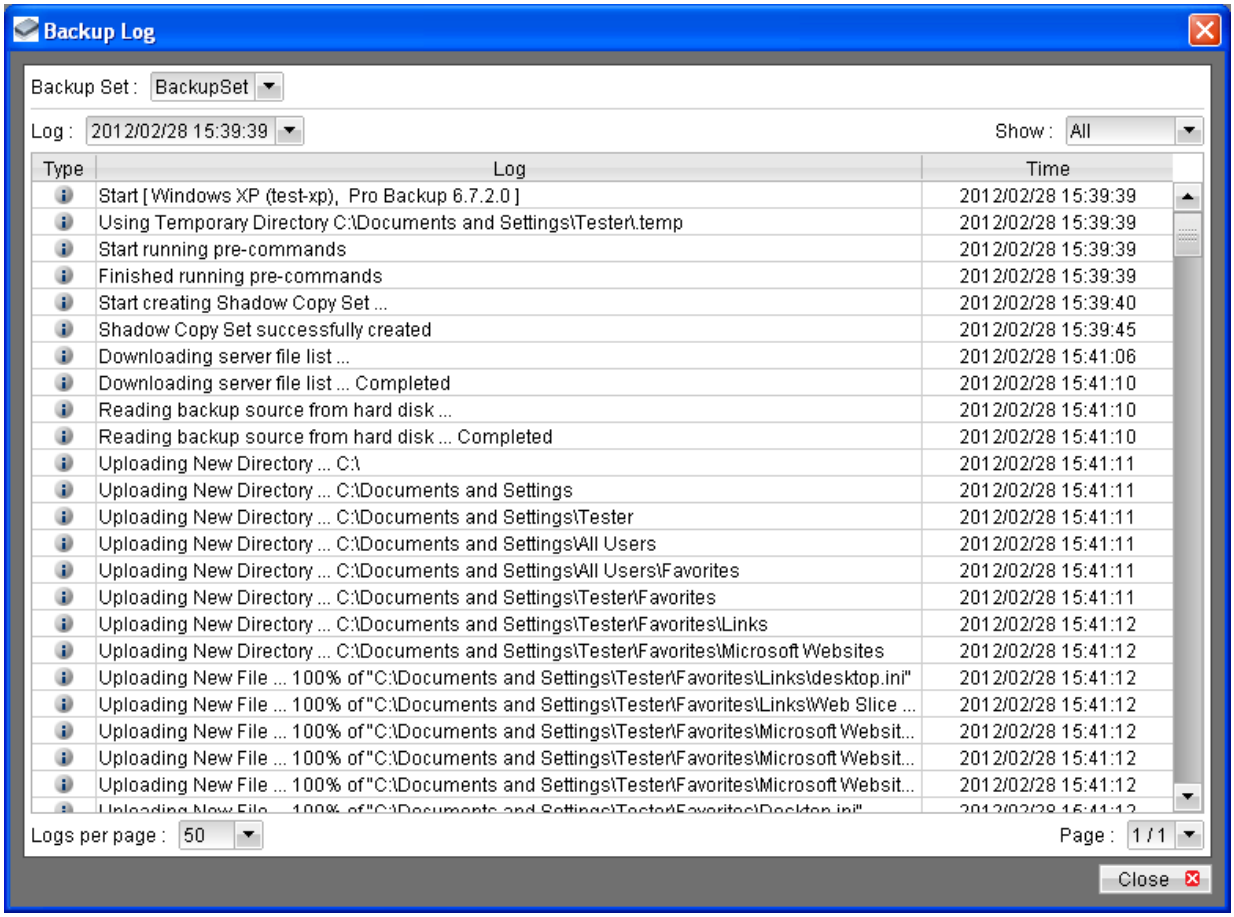


5.5 About Online Backup Manager

Click on the [About Online Backup Manager] button to view information of your backup application, such as the application version, and backup service provider's information like company name, website, email address and server hostname or IP address.

5.6 Backup Log

All backup activities are logged to a corresponding log files. To review them, click on the [Backup Log] button.

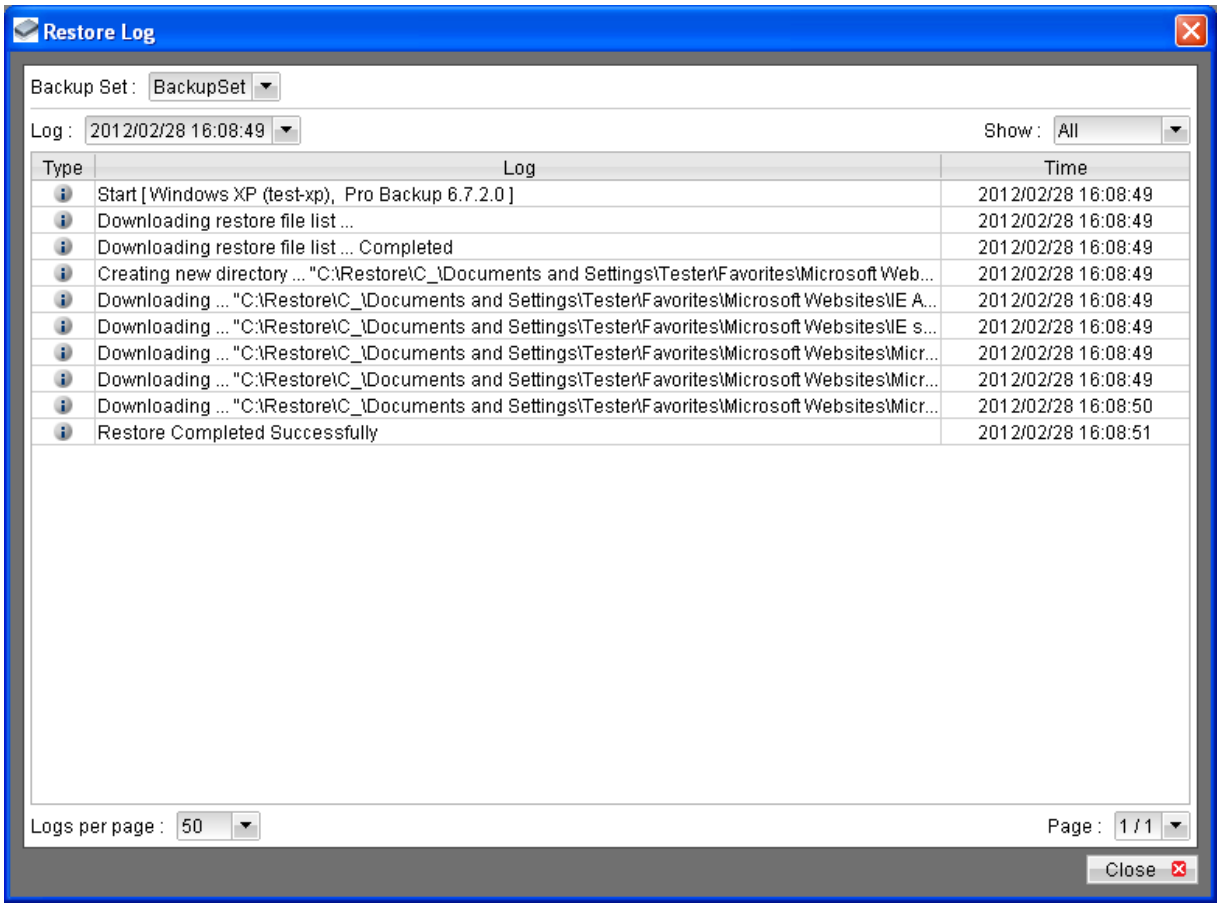

Backup Log
Backup Set : BackupSet
Log : 2012/02/28 15:39:39
Show : All
Type
Log
Time
Start [Windows XP (test-xp), Pro Backup 6.7.2.0] 2012/02/28 15:39:39
Using Temporary Directory C:\Documents and Settings\Tester\.temp 2012/02/28 15:39:39
Start running pre-commands 2012/02/28 15:39:39
Finished running pre-commands 2012/02/28 15:39:39
Start creating Shadow Copy Set ... 2012/02/28 15:39:40
Shadow Copy Set successfully created 2012/02/28 15:39:45
Downloading server file list ... 2012/02/28 15:41:06
Downloading server file list ... Completed 2012/02/28 15:41:10
Reading backup source from hard disk ... 2012/02/28 15:41:10
Reading backup source from hard disk ... Completed 2012/02/28 15:41:10
Uploading New Directory ... C:\ 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings\Tester 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings\All Users 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings\All Users\Favorites 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings\Tester\Favorites 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings\Tester\Favorites\Links 2012/02/28 15:41:12
Uploading New Directory ... C:\Documents and Settings\Tester\Favorites\Microsoft Websites 2012/02/28 15:41:12
Uploading New File ... 100% of "C:\Documents and Settings\Tester\Favorites\Links\desktop.ini" 2012/02/28 15:41:12
Uploading New File ... 100% of "C:\Documents and Settings\Tester\Favorites\Links\Web Slice ... 2012/02/28 15:41:12
Uploading New File ... 100% of "C:\Documents and Settings\Tester\Favorites\Microsoft Websit... 2012/02/28 15:41:12
Uploading New File ... 100% of "C:\Documents and Settings\Tester\Favorites\Microsoft Websit... 2012/02/28 15:41:12
Uploading New File ... 100% of "C:\Documents and Settings\Tester\Favorites\Microsoft Websit... 2012/02/28 15:41:12
Logs per page : 50
Page : 1 / 1
Close

Menu Item	Description
Backup Set	**Drop down menu for selecting which backup set.**
Log	**Drop down menu for selecting which log to review (in YYYY/MM/DD hh:mm:ss format).**
Show	**Drop down menu to filter display of only Information, Warning, Error, or all log entries.**
Logs per page	**Drop down menu for selecting the number of log entries to display per page.**
Page	**Drop down menu to switch the page number.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

5.7 Restore Log

Similar to backup, all restore activities are also logged to a corresponding log files. To review them, click on the [Restore Log] button.


Restore Log
Backup Set : BackupSet
Log : 2012/02/28 16:08:49
Show : All
Type
Log
Time
Start [Windows XP (test-xp), Pro Backup 6.7.2.0] 2012/02/28 16:08:49
Downloading restore file list ... 2012/02/28 16:08:49
Downloading restore file list ... Completed 2012/02/28 16:08:49
Creating new directory ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Web... 2012/02/28 16:08:49
Downloading ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Websites\IE A... 2012/02/28 16:08:49
Downloading ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Websites\IE s... 2012/02/28 16:08:49
Downloading ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Websites\Micr... 2012/02/28 16:08:49
Downloading ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Websites\Micr... 2012/02/28 16:08:49
Downloading ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Websites\Micr... 2012/02/28 16:08:50
Restore Completed Successfully 2012/02/28 16:08:51
Logs per page : 50
Page : 1 / 1
Close

Menu Item	Description
Backup Set	**Drop down menu for selecting which backup set.**
Log	**Drop down menu for selecting which log to review (in YYYY/MM/DD hh:mm:ss format).**
Show	**Drop down menu to filter display of only Information, Warning, Error, or all log entries.**
Logs per page	**Drop down menu for selecting the number of log entries to display per page.**
Page	**Drop down menu to switch the page number.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

6 Configure backup sets

This chapter describes how to configure a backup set.

A backup set defines the configuration of a backup routine, such as backup schedule, backup source and encryption setting as well as other options.

6.1 Backup Setting

Click on the [Backup Setting] button to:

- Create new backup set –

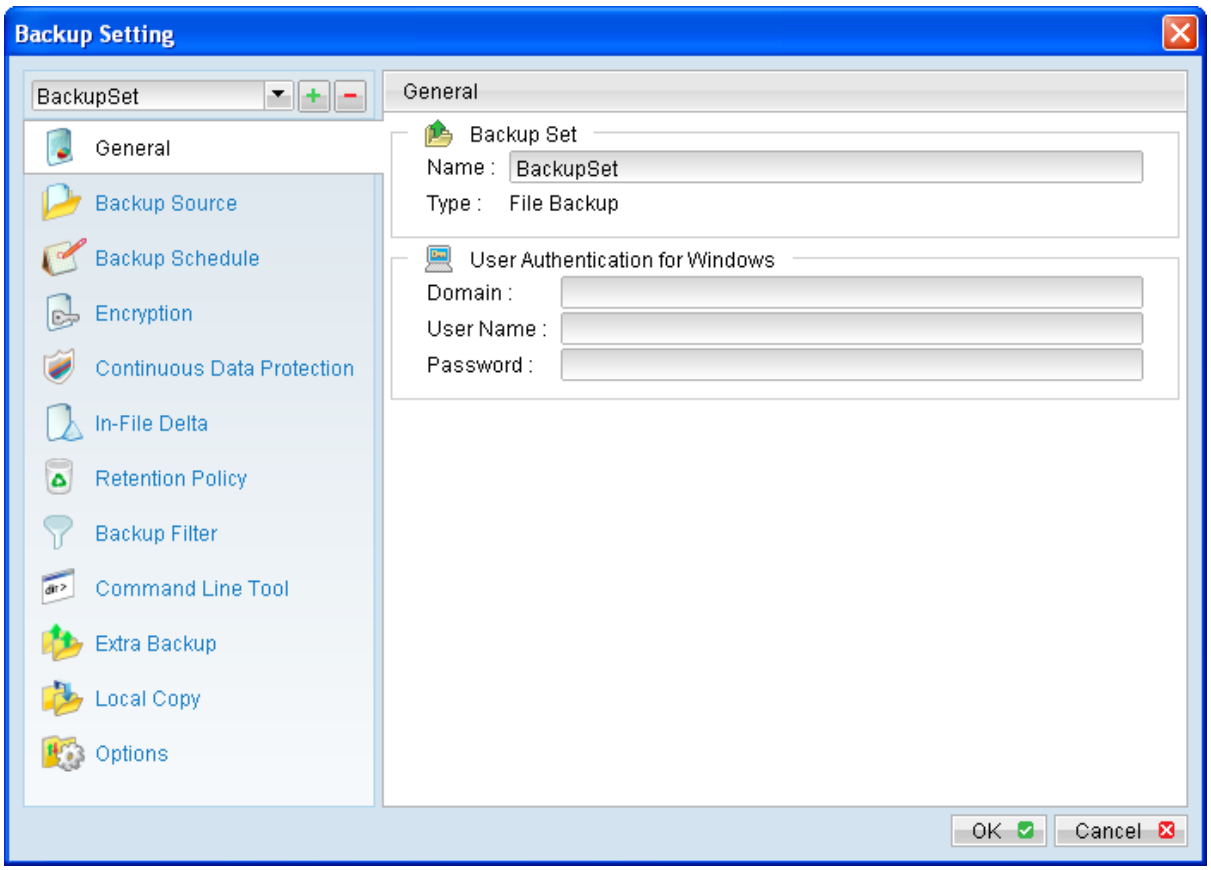
  Select the button to add a new backup set.

- Delete existing backup set –

  Select a backup set from the drop down menu, and the button to remove corresponding backup set.

- Modify existing backup set –

  Select a backup set from the drop down menu, and other options from the left panel to modify the backup set.



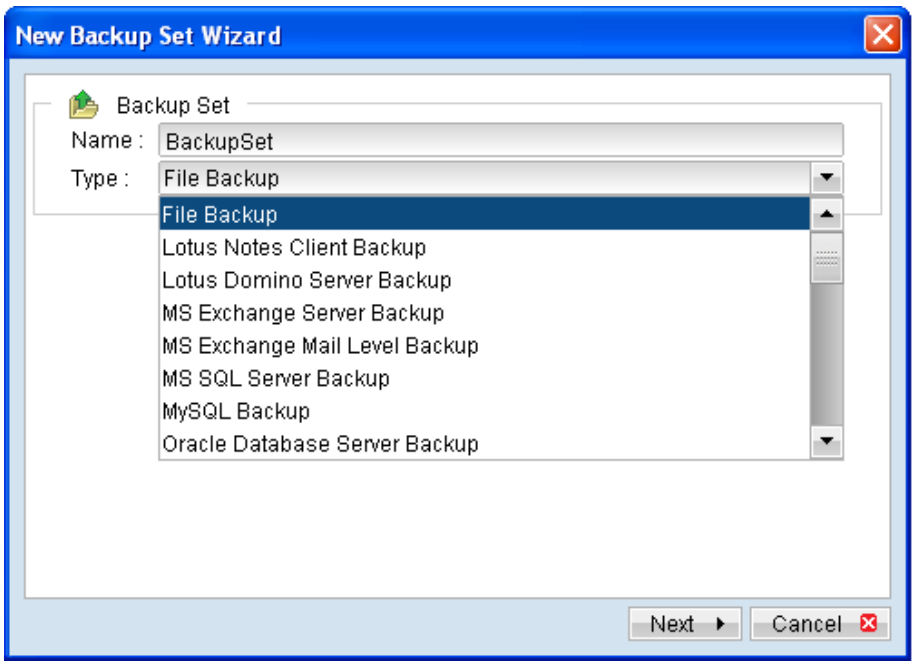
Icon	Menu Item	Description
	General	**Click to access the general backup set menu.**
	Backup Source	**Click to access the backup source selection menu.**
	Backup Schedule	**Click to access the backup schedule setting menu.**
	Encryption	**Click to access the encryption setting menu.**
	Continuous Data Protection	**Click to access the continuous data protection menu.**
	In-File Delta	**Click to access the In-file delta menu.**
	Retention Policy	**Click to access the retention policy menu.**
	Backup Filter	**Click to access the backup filter menu.**

	Command Line Tool	**Click to access the pre post command line tool menu.**
	Extra Backup	**Click to access the extra backup setting menu.**
	Local Copy	**Click to access the local copy backup menu.**
	Options	**Click to access the option menu.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

6.1.1 New Backup Set Wizard

Select the button to start the New Backup Set Wizard.



Select the corresponding backup type, in this case, a file backup set.

A backup set can be one of the following types:

Backup Type	Description
File	**Backup set type for backup of normal files.**
Lotus Domino Server	**Backup set type for backup of Lotus Domino server.**

Lotus Notes Client	**Backup set type for backup of Lotus Notes client.**
MS Exchange Server	**Backup set type for backup of Microsoft Exchange server.**
MS Exchange Mail Level	**Backup set type for backup of individual emails (brick level backup).**
MS SQL Server	**Backup set type for backup of Microsoft SQL server.**
MySQL Server	**Backup set type for backup of backup MySQL server.**
Oracle Database Server	**Backup set type for backup of Oracle database server**
System State	**Backup set type for backup of Microsoft Window's System State.**
ShadowProtect System	**Backup set type for Bare-Metal backup of your system using StorageCraft's ShadowProtect.**
Windows System	**Backup set type for Bare-Metal backup of your system using Microsoft's WBAdmin.**
MS VM	**Backup set type for backup of Virtual Machine on Microsoft Hyper-V server.**
VMware VM	**Backup set type for backup of Virtual Machine on VMware server (VM Server, ESX, ESXi ... etc).**

*The availability of backup type listed above may be service provider dependent. If a backup type is not available, please check with your service provider for further details and availability.

For exact application support list, please contact your service provider for further details.

Note:
Backup set type is defined at the backup set creation time, and **cannot be modified afterward**.

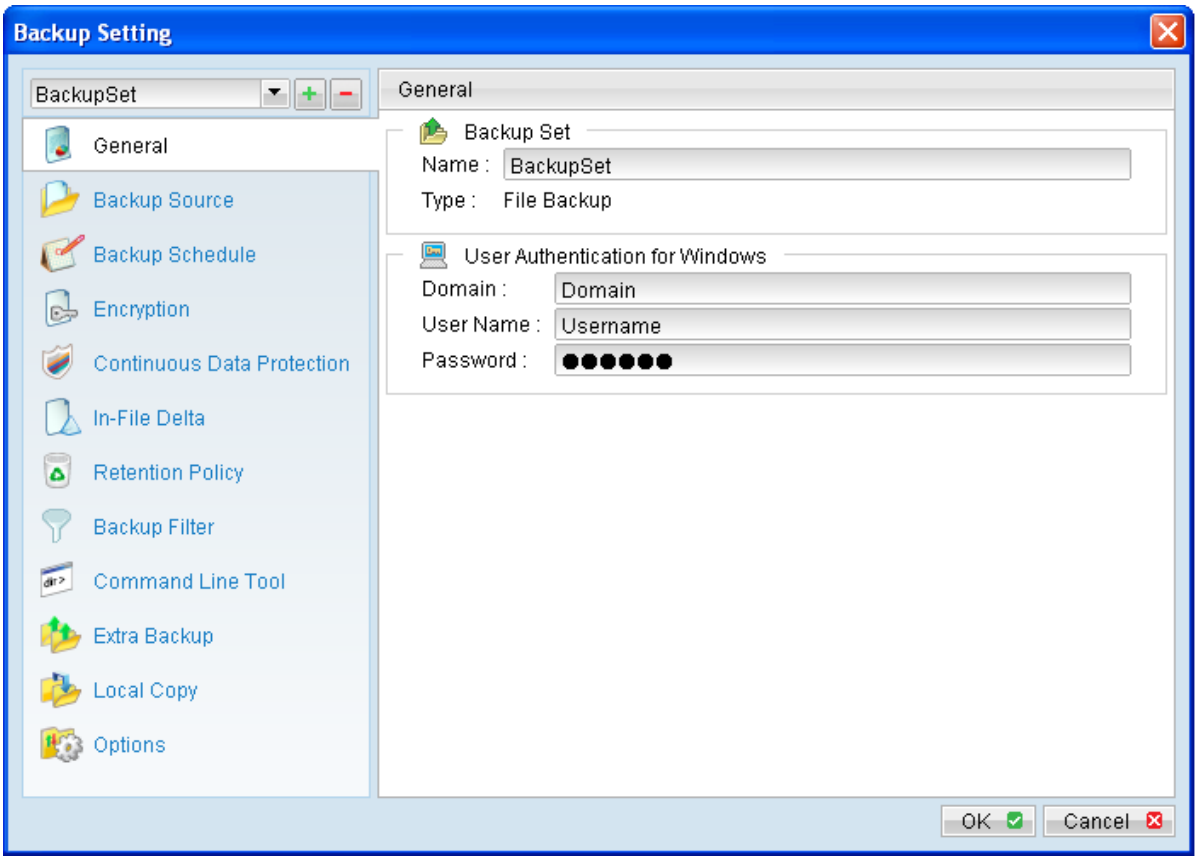
Next few steps of a new backup set creation process, including Backup Source, Backup Schedule and Encryption setting configuration are discussed in the following sections of the guide.

6.1.2 General

Click on the [General] tab to modify the [Backup Set Name] or [User Authentication for Windows] setting.

For backup set with backup schedule and network shared drive selected as backup source, the [User Authentication for Windows] is a **mandatory field** that must be filled in.

Please specify a Windows domain account for the backup client application with sufficient permission to access the network location.



Menu Items	Description
Domain	**Input box for entering domain of the Windows domain account.**
User Name	**Input box for entering username of the Windows domain account.**
Password	**Input box for entering password of the Windows domain account.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

6.1.3 Backup Source

Click on the [Backup Source] tab to configure backup source of a backup set.

A Backup Source defines the files and directories to be included for backup.

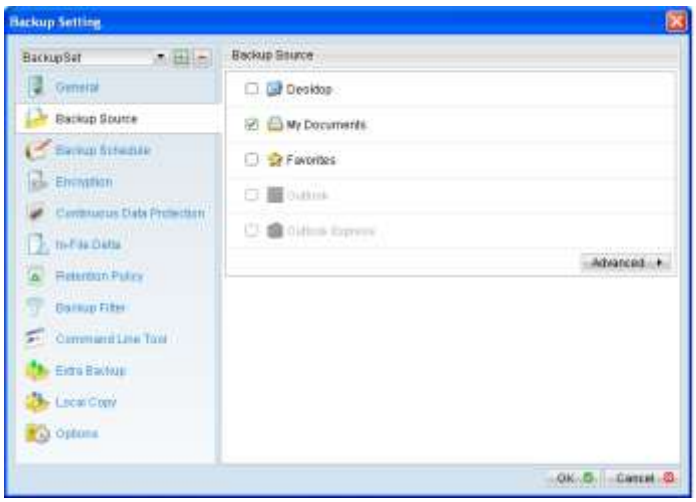
There are two types of backup source: Selected and Deselected.

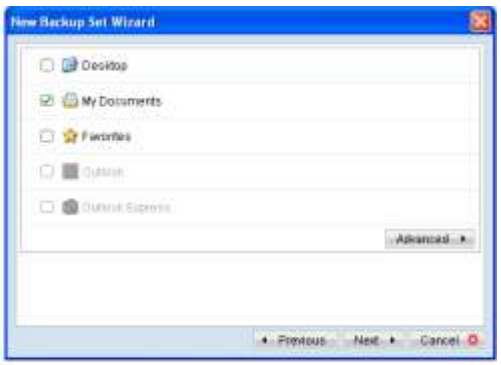
- Selected backup source defines files and directories that are to be included in a backup set.

- Deselected backup source defines files and directories that are to be excluded from a backup set.

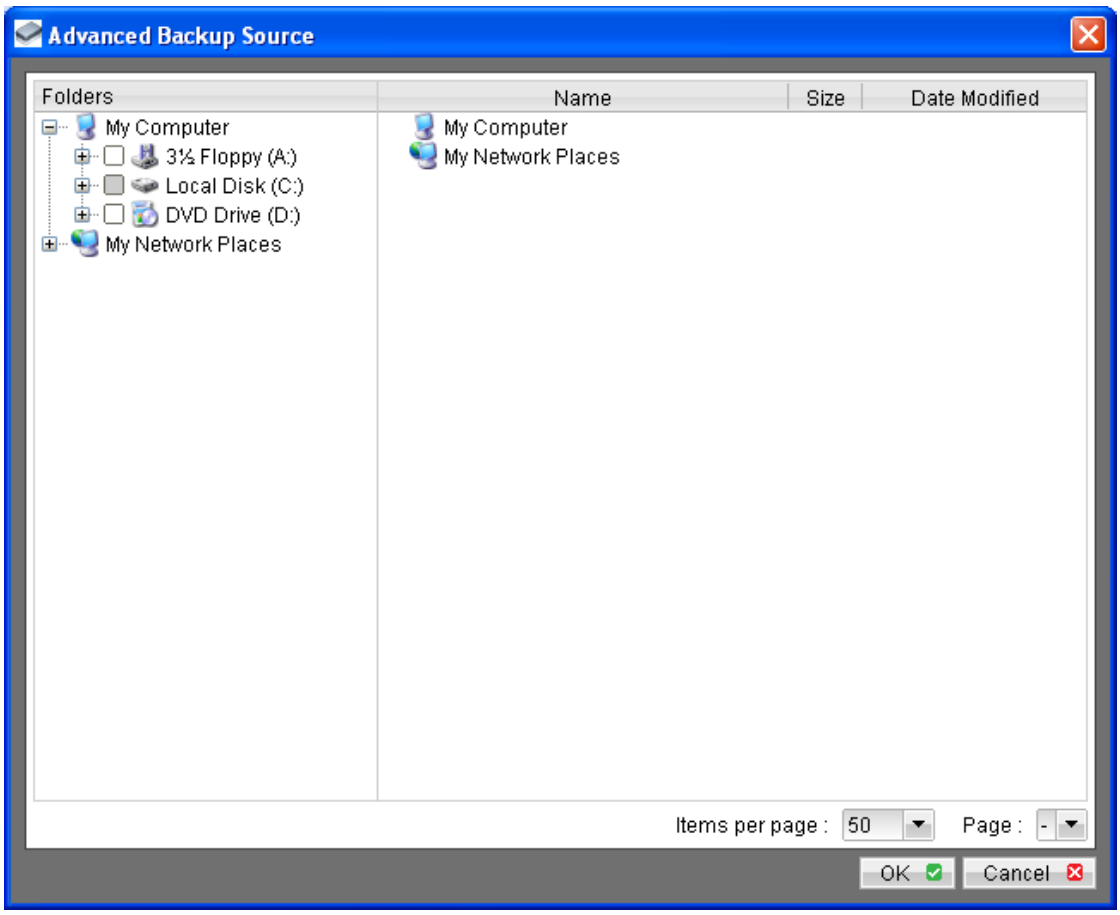
On the basic backup source selection dialog, you can select directories that are commonly selected as backup source for backup:

- Desktop folder
- My Documents folder
- Favorites folder
- Outlook and Outlook Express folder





Click on [Advanced] button to access the advanced backup source dialog to select other directories for backup.



The checkbox beside a root drives, directory or file can be in one of the following mode:

Mode	Description
☑	**All directories and files under this directory will be backed up.**
☑	**All directories and files under this directory except those explicitly excluded will be backed up.** **Directories and files selected to this directory in the future will be backed up as well.**
☐	**Only the checked directories and files under this directory will be backed up.** **Directories and files selected to this directory in the future will not be backed up.**
☐	**No directory or file under this directory will be backed up.**

Note:

For installation on Windows platforms, hidden directories and files will be displayed only if the [Hide protected operating files] setting of Windows Explorer is disabled.

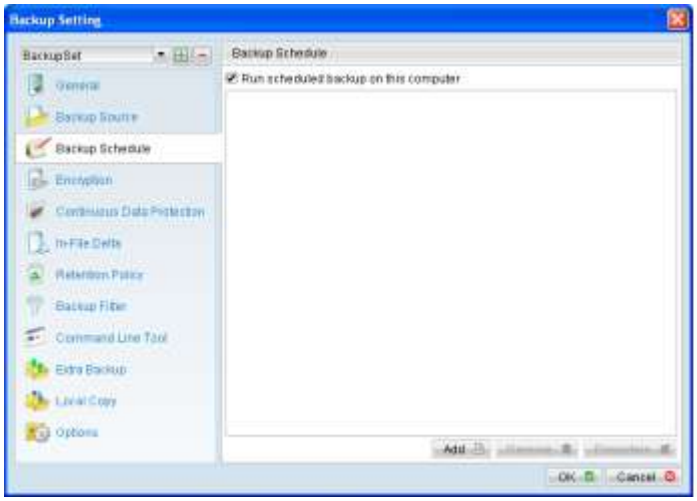
By selecting a parent directory as backup source, all child directories and files including any hidden directories or files would be backup as well.

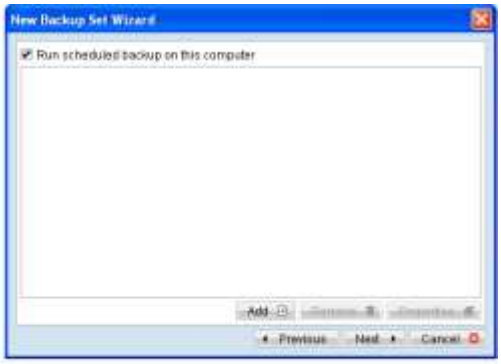
To avoid backing up hidden directories such as the Recycle Bin folder, please select the corresponding directories or files required as backup source directly, instead of selecting the parent directory or root drive letter.

6.1.4 Backup Schedule

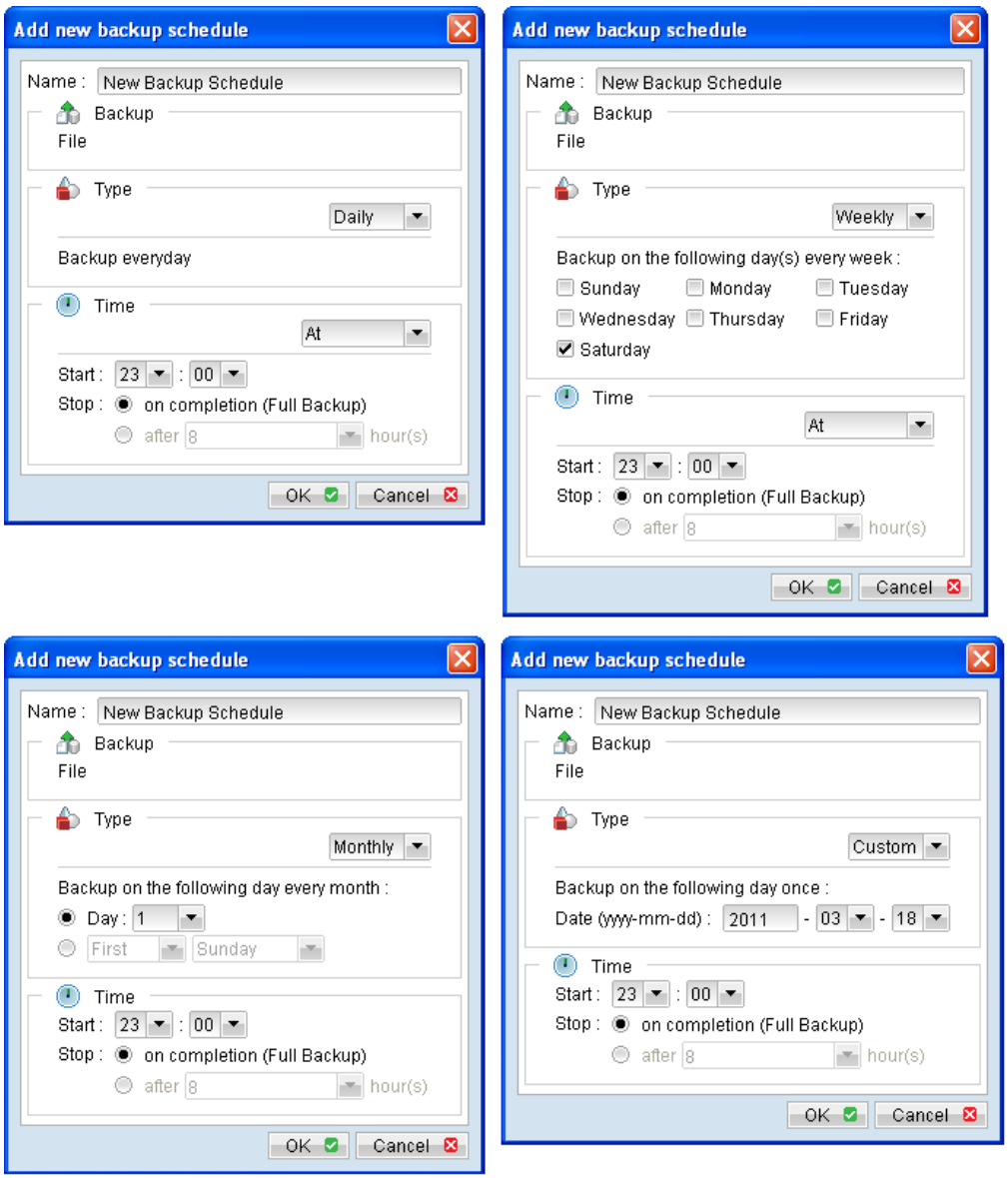
Click on the [Backup Schedule] tab of the backup setting menu to configure backup schedule of a backup set.

A Backup Schedule defines the time, time period allowed, and frequency that backup job for an existing backup set should be run automatically.





Menu Items	Description
Run scheduled backup on this computer	**Checkbox to enable or disable the corresponding backup set to run on this computer.**
Add	**Click to add a new backup schedule.**
Remove	**Click to remove an existing backup schedule.**
Properties	**Click to modify an existing backup schedule.**



Menu Items	Description
Name	**Input box for entering backup schedule name.**
Type	**Checkbox to select schedule type.** **Daily - Backup job will run everyday at a specific time under this schedule type** **Weekly - Backup job will run on specific day(s) of a week, at a specific time under this schedule type.** **Monthly - Backup job will run on specific day of a month (date, or special criteria such as**

	first weekend, last weekday), at a specific time under this schedule type. **Custom - Backup job will run on specific day of a year (date), at a specific time under this schedule type.**
Time (At)	**To start backup job at a specific time.** **Start - Dropdown menu to select the start time of a backup job.** **Stop – Option to allow a backup job to run to completion, or to stop the running backup job after a specified hour.**
Time (Periodically)	**To start backup job at regular intervals of time.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

To configure a Daily backup schedule where backup job will run everyday at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Daily] from the schedule [Type] dropdown menu.
4. Select [At] from the [Time] dropdown menu.
5. Configure start time to be 20:00
6. Configure the stop option according to your requirement.

To configure a Weekly backup schedule where backup job will run on Friday every week at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Weekly] from the schedule [Type] dropdown menu.
4. Select the checkbox beside [Friday].
5. Select [At] from the [Time] dropdown menu.
6. Configure start time to be 20:00
7. Configure the stop option according to your requirement.

To configure a Monthly backup schedule where backup job will run on first weekend of every month at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.

3. Select [Monthly] from the schedule [Type] dropdown menu.
4. Select [First], [Weekend].
5. Select [At] from the [Time] dropdown menu.
6. Configure start time to be 20:00
7. Configure the stop option according to your requirement.

To configure a Custom backup schedule where backup job will run on Jan 1st of 2012 (2012-01-01) at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Custom] from the schedule [Type] dropdown menu.
4. Enter the date when the backup should be performed (YYYY-MM-DD).
5. Configure start time to be 20:00
6. Configure the stop option according to your requirement.

Note that multiple backup schedules of different type (e.g. daily, weekly) can also be configured for a single backup set.

For example:

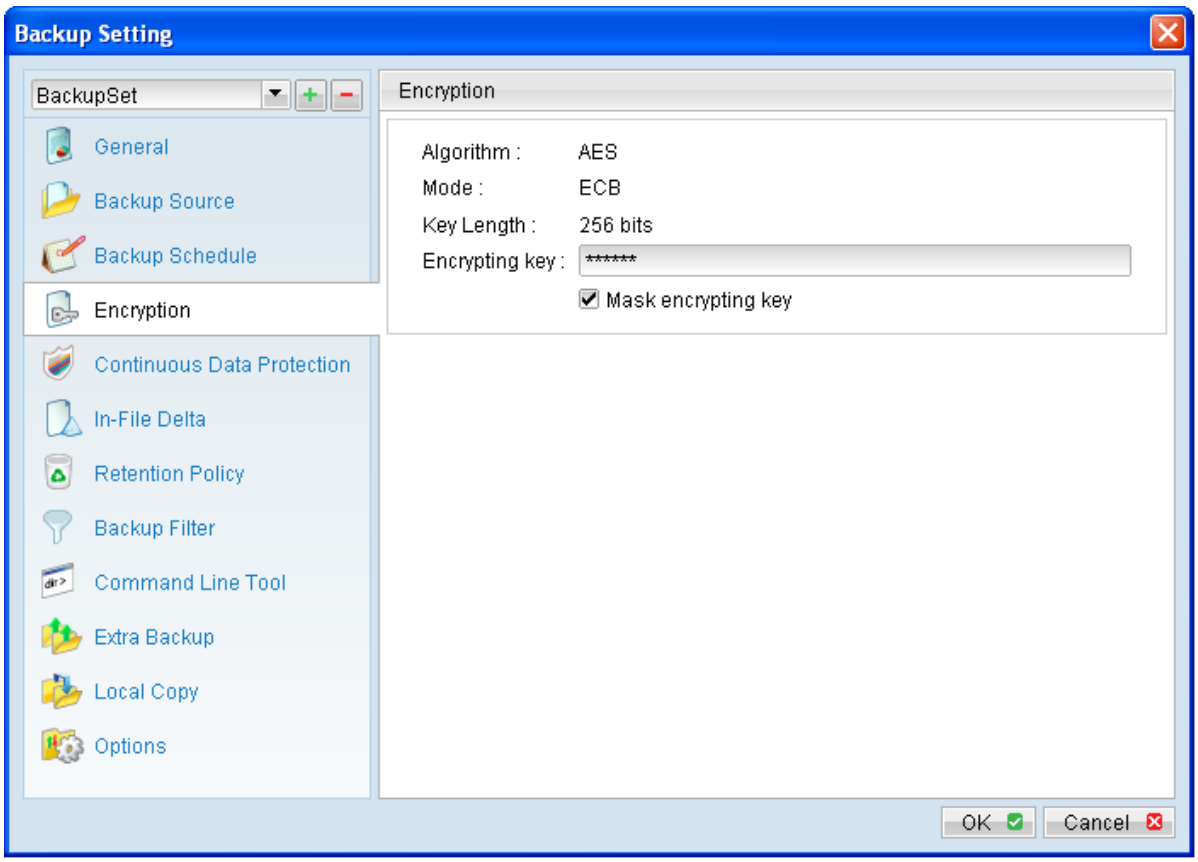
- Daily backup schedule at 00:00
- Daily backup schedule at 12:00
- Weekly backup schedule on Friday at 18:00

Combination of these schedules effectively creates a schedule for backup at 00:00 and 13:00 everyday, and 18:00 every Friday.

6.1.5 Encryption

Before files are uploaded to the backup server, they are first compressed and encrypted with an algorithm, mode and key of your choice.

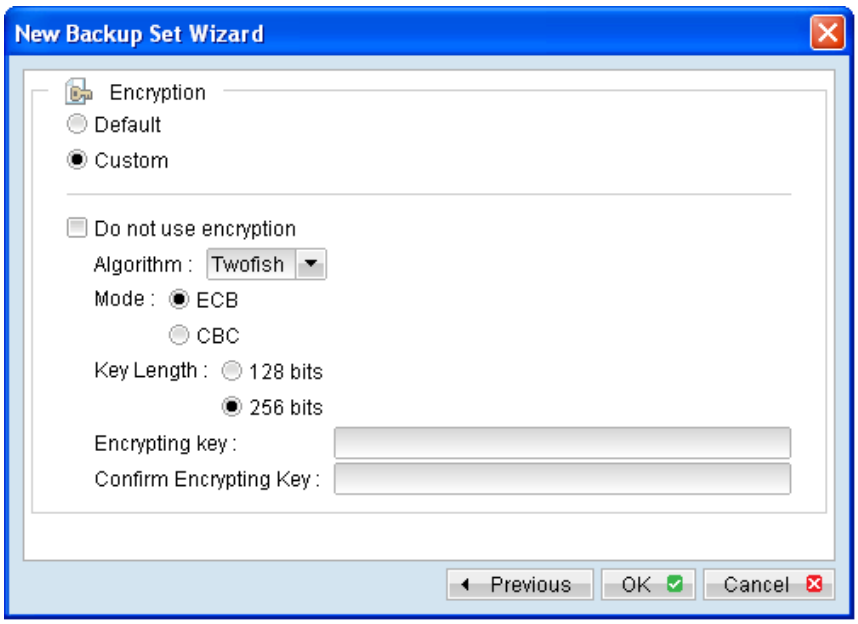
Select the [Encryption] tab to view the current encryption setting of an existing backup set.



Menu Items	Description
Encryption key	**Text box displaying the encryption key for the corresponding backup set.**
Mask encryption key	**Checkbox to enable or disable masking of the encrypting key.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Encryption settings are set at a backup set's creation time in the New Backup Set Wizard.



Menu Items	Description
Default	**Radio button to select default encrypting key.** **Default encryption setting -** **Encryption algorithm: AES** **Encryption mode: ECB** **Key Length: 256 bits** **Encrypting key: Same as current password**
Custom	**Radio button to select your custom encryption setting, including:** **Encryption algorithm** **Encryption mode** **Key Length** **Encrypting key**
Do not use encryption	**Checkbox to disable encryption (not recommended).**
Algorithm (used with Custom)	**Dropdown menu to select the encryption algorithm setting:** **Twofish - Twofish algorithm** **DESede - Triple DES algorithm** **AES - Advanced Encryption Standard algorithm**
Mode (used with Custom)	**Radio button to select ECB or CBC encryption mode:**

	ECB - Electronic Cook Book mode **CBC - Cipher Block Chaining mode**
Key Length (used with Custom)	**Radio button to select 128 bit or 256 bit key length.**
Encrypting key (used with Custom)	**Input box for entering your choice of encrypting key.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Select [Default] encryption setting if you are not familiar with encryption algorithm or mode. The default encryption setting is:

Encryption Algorithm: AES
Encryption Mode: ECB
Key Length: 256 bits
Encrypting Key: Same as current password

Encryption settings are set at a backup set's creation time and cannot be modified afterward.

If custom encrypting key is used, please considering the following to create a strong encrypting key:

- Length
  Make sure the encryption key is at least eight or more characters.

- Complexity
  Include lowercase, uppercase letters and numbers, use the entire keyboard not just the letters and characters you use or see most often.

Avoid creating encryption key that uses:

- Dictionary words.

- Words spelled backwards, common misspellings and abbreviations.

- Sequence or repeated characters.

- Personal information, your name, your birthday, or similar information. Include letters and numbers, use the entire keyboard not just the letters and characters you use or see most often.

Important:
By selecting default encryption setting, password string of the backup account will be configured as encrypting key for the corresponding backup set.

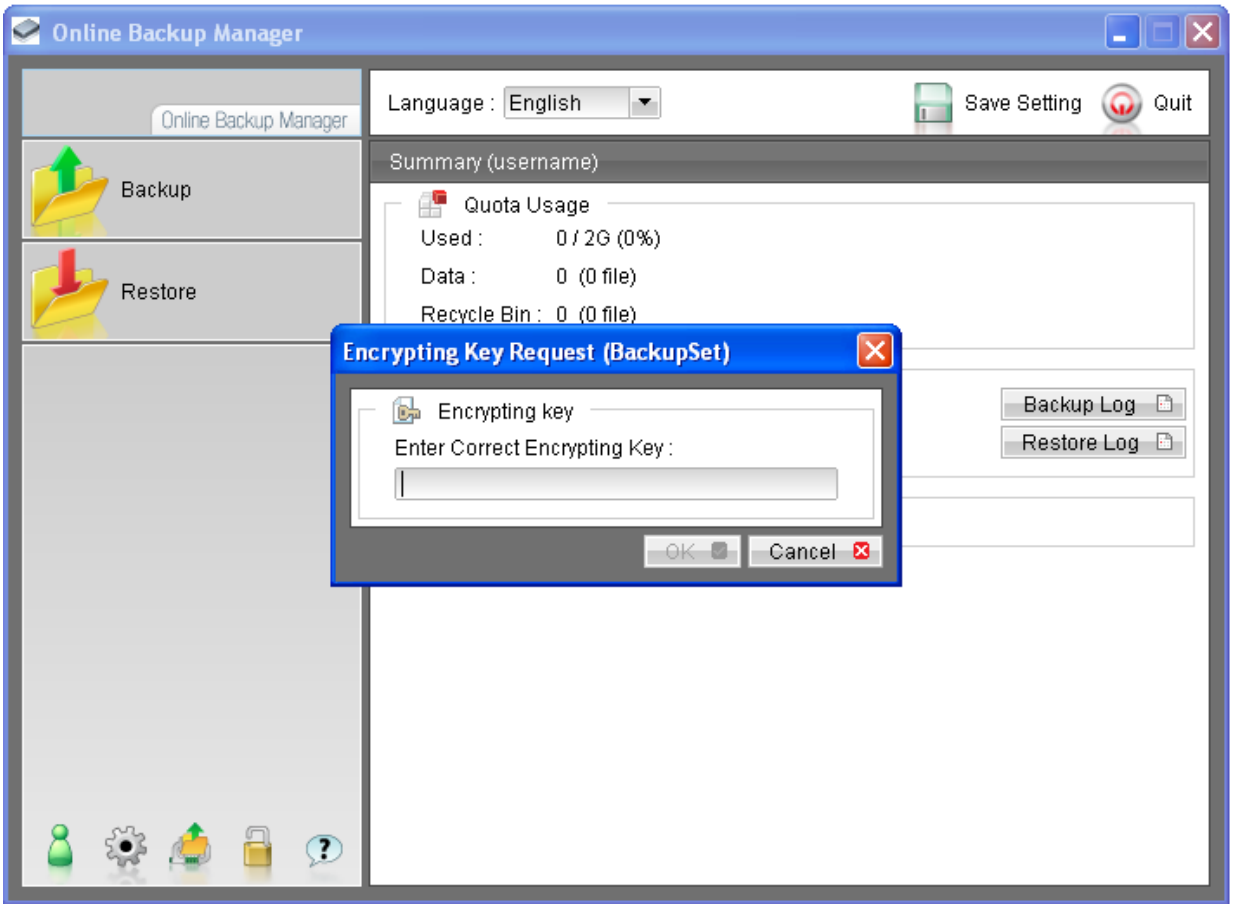
The encryption key is independent from a backup account's password.

Encryption settings are set at a backup set's creation time, even if the password is changed afterward, the encryption key remain the same.

It is **very important** that the encryption key is written down, and additional copies of the key are made, and stored in safe places so that it is readily available when needed to restore data.

If the encryption key is lost, the data is irretrievable.

For initial login of existing backup user on new computer, you will be prompted for the encrypting key of all existing backup set.



Menu Item	Description
Enter Correct Encrypting Key	**Input box for entering encrypting key of existing backup set.**
OK	**Click to confirm on encrypting key.**
Cancel	**Click to proceed without using encrypting key.**

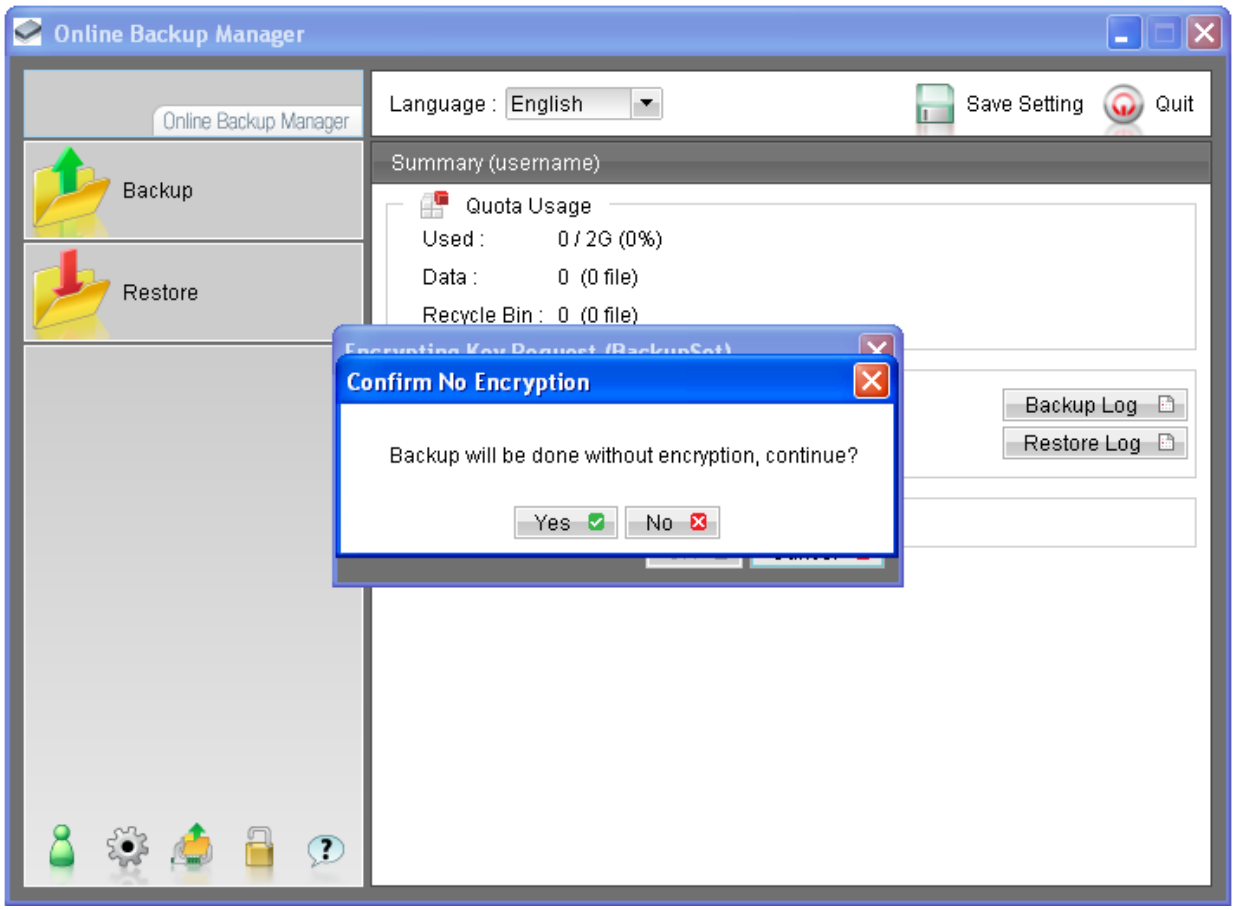
Enter the correct encrypting key and click [OK] to proceed.

Alternatively, press [Cancel] to proceed (e.g. if the encrypting key is lost) without encryption, for all backup job performed afterward.

A confirmation box will be prompted to confirm.

By continuing without encryption, it allows data backed up in the future to be restorable (they are no longer encrypted).

However, existing data that are encrypted by the lost encrypting key would not be restorable.

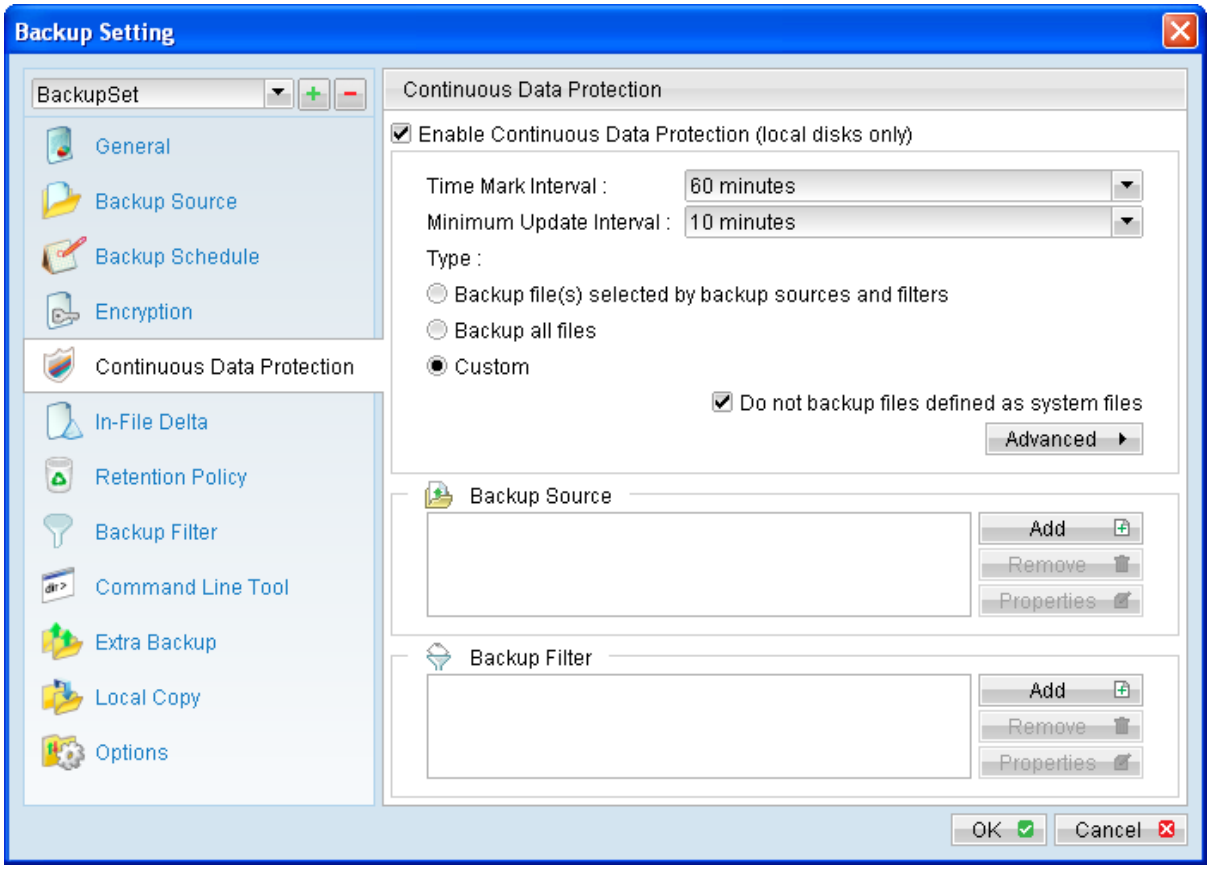


Important:
In the event of lost encrypting key, it is strongly recommended that a new backup set be created. This ensures that data backed up in the future are both encrypted and restorable.

6.1.6 Continuous Data Protection (CDP)

Continuous Data Protection (CDP) is a feature providing backup for selective data whenever change is made. Depending on the option selected, every version of a file is backed up close to real time.

To enable CDP, click on the [Continuous Data Protection] tab and select the [Enable Continuous Data Protection] checkbox.



Menu Items	Description
Enable Continuous Data Protection	**Checkbox to enable or disable CDP.** **Note:** **CDP will only backup directories and files on local drive, but not on floppy drive, removable drive or network drive.**
Time Mark Interval	**Defines a regular interval of time (e.g. every x minutes), with each interval containing one snapshot (the first backup of each interval)**

	available for restore. **For example, for [Time Mark Interval] set to 60 minutes, with the file updated every 5 minutes. A restore-able snapshot of the file will be available for each interval:** **00:05, 01:05, 02:05, 03:05 ... etc.**
Minimum Update Interval	**Defines how often an updated file is backed up to the backup server.** **For example, for [Minimum Update Interval] set to [Always], file will be backed up to the server as they are updated.**
Backup file(s) selected by backup sources and filters	**Radio button to select if CDP will only backup modified directories or files selected as backup source.**
Backup all files	**Radio button to select if CDP will back up all modified directories and files on all local drive.**
Custom	**Radio button to select if CDP will backup a custom set of directories and files.** **Note: This custom set of directories and files can be different than the backup source selected for the backup set.**
Backup Source (used with Custom)	**Add – Click to select a custom set of directory or file as backup source for CDP backup.** **Remove – Click to remove a selected directory or file as backup source for CDP backup.** **Properties – Click to modify a selected directory or file as backup source for CDP backup.**
Backup Filter (used with Backup all files or Custom)	**Add – Click to create a backup filter for CDP backup.**

	Remove – Click to remove a backup filter for CDP backup. **Properties – Click to modify a backup filter for CDP backup.** **Note: Backup filter is case sensitive.**
Do not backup files defined as system files	**When this option is enabled, CDP will automatically exclude the following files from its backup:** **C:\hiberfil.sys** **C:\Pagefile.sys** **C:\Program Files*** **C:\RECYCLER** **C:\System Volume Information** **C:\Windows*** **${App_Data}\Avg7** **${App_Data}\Avg8** **${App_Data}\Kaspersky Lab** **${App_Data}\McAfee** **${App_Data}\McAfee.com** **${App_Data}\Microsoft** **${App_Data}\Sophos** **${App_Data}\Symantec** ****.tmp** ***\Application Data\Macromedia*** ***\Application Data\Mozilla*** ***\Local Settings\Application Data\Microsoft*** ***\ntuser.dat**
Advanced	**Click to access advanced CDP backup control to backup only when:** **CPU usage is less than a specific percentage.** **Network traffic is less than a specific Megabyte per second.** **No keyboard or mouse input exceeding a specific time (in minute).**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Note:
The [Continuous Data Protection] tab is only available for OBM installation in Windows platforms.

Configure the [Time Mark Interval] and [Minimum Update Interval] according to your recovery requirement.

Time mark interval defines a regular interval of time, where each interval contains one snapshot available for restore.

For example, when [Time Mark Interval] is configured to 60 minutes. 24 intervals would be marked per day, with each interval spanning across 60 minutes:

Interval 1 – 00:00 to 01:00
Interval 2 – 01:00 to 02:00
Interval 3 – 02:00 to 03:00
Interval 4 – 03:00 to 04:00

To

Interval 23 – 22:00 to 23:00
Interval 24 – 23:00 to 24:00

Assuming that a file is backed up multiple times (by CDP) within each interval, the first backup (e.g. snapshot) of each interval would be available for restore.

Minimum update interval defines the minimum period of time before an updated file is backed up to the backup server.

For example, when [Minimum Update Interval] is configured to 10 minutes, updated file would be backed up to the backup server every 10 minutes. To ensure that updated files are always uploaded to the server immediately, you can consider setting the [Minimum Update Interval] as Always.

To configure CDP for backup of the **directories and files selected as backup source**:

1. Select the [Backup file(s) selected by backup sources and filters] radio button for [Type].

To configure CDP for backup of **all local drive(s)**:

1. Select the [Backup all files] radio button for [Type].
2. Configure [Backup Filter] for inclusion or exclusion of file if necessary.

To configure CDP for backup of a **custom set of directories or files**:

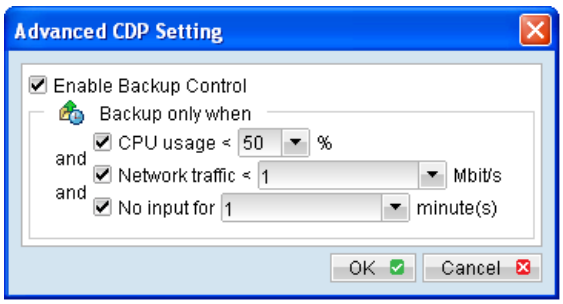
1. Select the [Custom] radio button for [Type].
2. Click [Add] beside the [Backup Source] section (within the CDP tab).
3. Select the custom set of data for backup.
4. Configure [Backup Filter] for inclusion or exclusion of file if necessary.

Note that the backup filter function is only available for CDP type [Backup all files] or [Custom].

Although CDP can be a helpful feature, the protection offered by CDP is often heralded without consideration of the disadvantages that it can present.

Specifically, the continuous CPU, memory and bandwidth usage can adversely affect the corresponding machine's performance.

To enable backup control for CDP backup, select [Advanced] to open the advanced CDP setting dialog:



To allow CDP backup only when CPU usage is under 50%:

1. Select the checkbox beside [CDP usage].
2. Select the corresponding percentage from the [%] dropdown menu.

To allow CDP backup only when network traffic is under 10 Mbit/s:

1. Select the checkbox beside [Network traffic]
2. Enter the corresponding number in the [Mbit/s] textbox.

To allow CDP backup only when there is no keyboard or mouse input for 5 minutes:

1. Select the checkbox beside [No input for].
2. Enter the corresponding number (in minutes) in the [minute(s)

Important:
Continuous Data Protection (CDP) will only backs up data selected as backup source after the CDP module is enabled. Existing data that are not updated will not be backed up by the CDP module.

Furthermore, CDP is not a replacement for the traditional schedule backup but works along with the scheduled backup to provide timely protection for your data.

CDP will automatically be stopped when a manual or scheduled backup is started, and will resume when the job is completed.

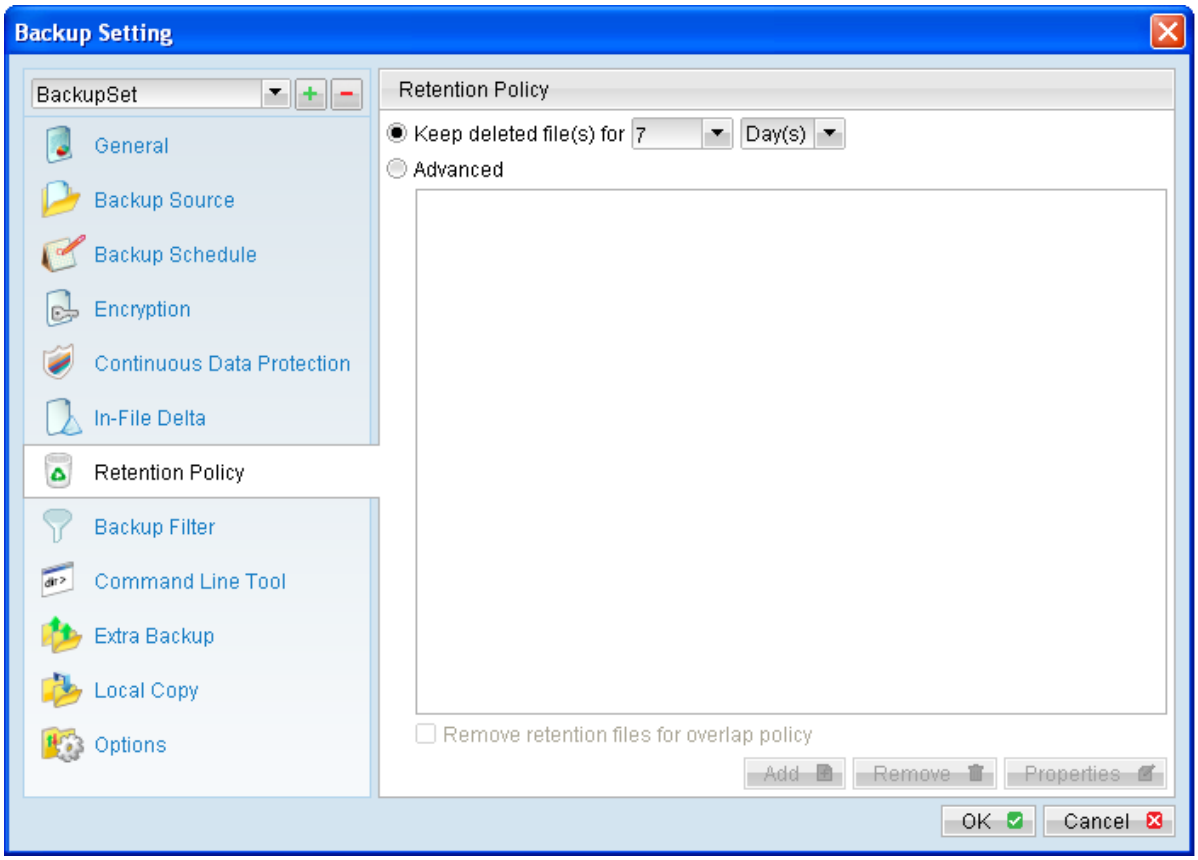
Note: It is not possible to run multiple CDP backup sets on the same machine with different backup user accounts.

6.1.7 In-File Delta

For more details about the In-file delta technology, please refer to the In-File Delta Technology section to be followed in this guide.

6.1.8 Retention Policy

Click on the [Retention Policy] tab to modify the retention policy of an existing backup set.



Retention policy defines the policies of persistent data management for meeting business data archival requirements.

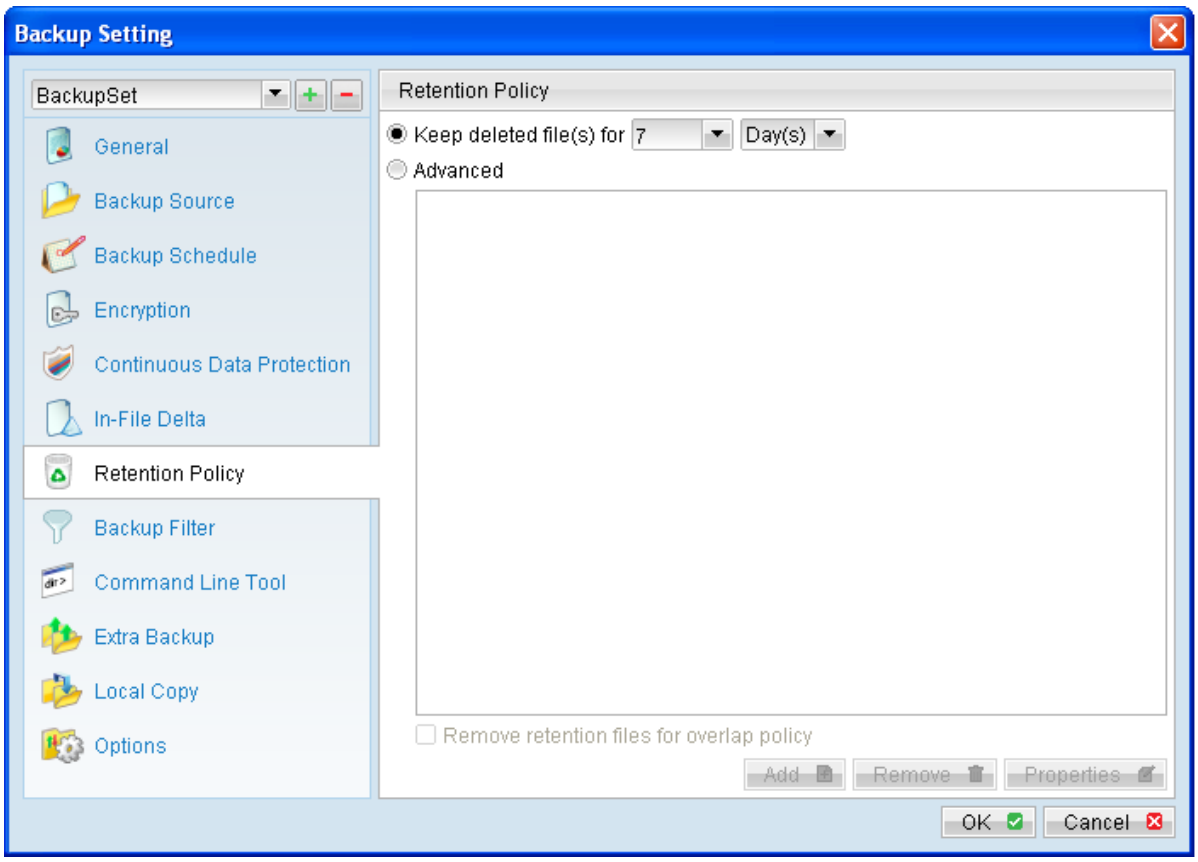
When a backup job is performed, for data that are modified or deleted on the client computer, their existing version on the backup server (backed up previously) would be moved into retention area, while newly backed up file would be placed in the current data area.

Specifically, retention policy setting defines how long are these data kept within the retention area before they are deleted permanently from the backup server.

For backed up data that have not been updated or deleted from the client computer, they are kept in the data area on the backup server and remain untouched.

A **standard retention policy** defines a basic policy where retained file (in the retention area) are removed automatically after a user specific number of days or backup jobs.

To define a standard retention policy, simply modify the [Keep delete file(s) for] drop down menu to your required days or jobs. Press [OK] and save before exiting the backup application to confirm the changes.



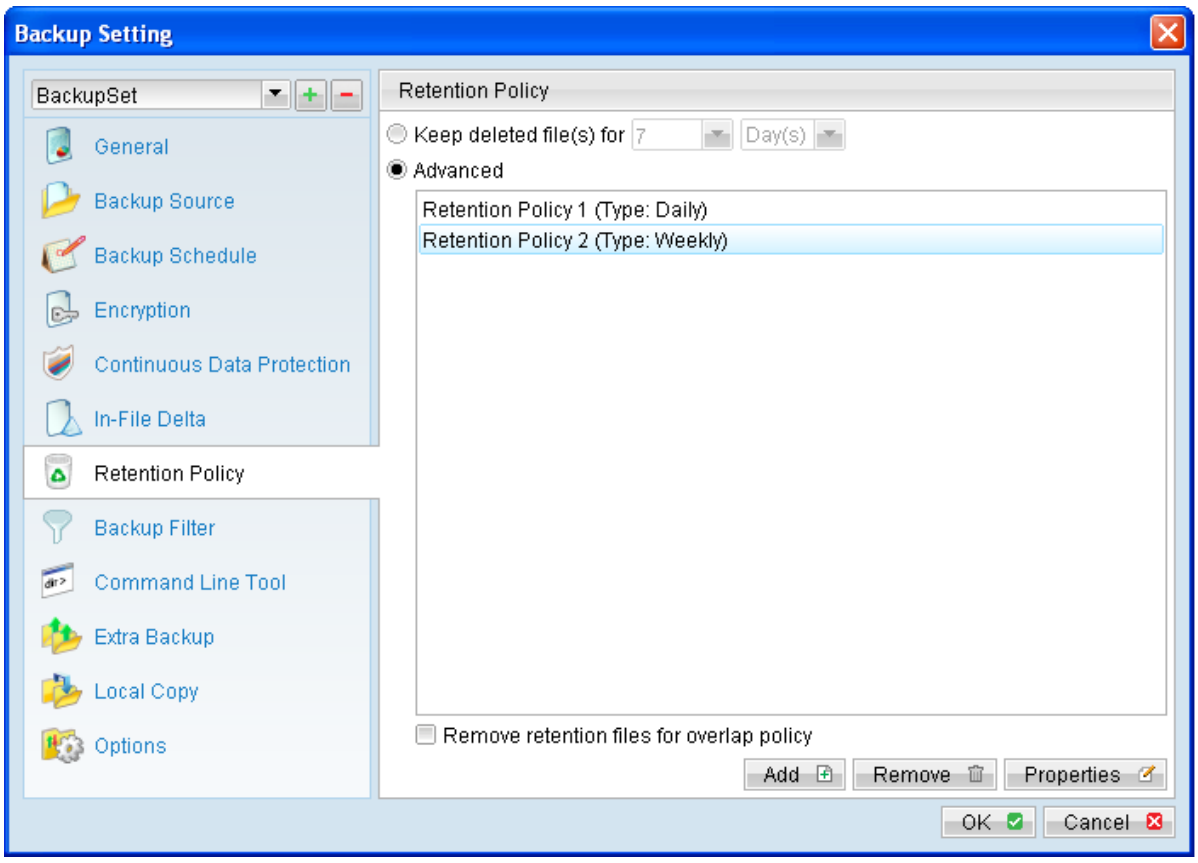
An **advanced retention policy** defines a more advanced and flexible policy where retained file (in the retention area) are removed automatically after a combination of user defined policy, such as:

- A specific number of days
- A specific number of weeks, including the day of the week
- A specific number of months, including the day of the month
- A specific number of years, including the day of the year

To define an advanced retention policy, select the [Advanced] button, and press the:

- [Add] button to add new policy
- [Remove] button to remove existing policy
- [Properties] to edit existing policy

Press [OK] and save before exiting the backup application to confirm the changes.



For example, you can configure the advanced retention policy to keep all data backed up:

- In the last 7 days.
- In the last 4 Saturdays.
- In the 1st day of each month in the last 3 months.
- In the 1st day of each quarter in the last 12 months.

- In the 1st day of each year in the last 7 years.

To achieve the above example policy, configured the advanced retention policy as follows:

- Type: **Daily**
  Number of snapshots to keep: **7**

- Type: **Weekly**
  Keep retention files for the following days: **Saturday**
  Number of snapshots to keep: **4**

- Type: **Monthly**
  Keep retention files for the following days: **Day 1**
  Number of snapshots to keep: **3**

- Type: **Quarterly**
  Keep retention files for the following days:
  Month - January, April, July, October
  Day 1
  Number of snapshots to keep: **4**

- Type: **Yearly**
  Keep retention files for the following days: **01-01**
  Number of snapshots to keep: **7**

Assuming that a file is updated and being backed up everyday for the past 7 hears, and today is January 11, 2011.

If the option [Remove retention files for overlap policy] is not enabled, a total of 22 snapshots (previous version) of the file would be available for restore:

Daily	Weekly	Monthly	Quarterly	Yearly
16-Jan-2011	**14-Jan-2011**	**01-Jan-2011**	**01-Jan-2011**	**01-Jan-2011**
15-Jan-2011	**07-Jan-2011**	**01-Dec-2010**	**01-Oct-2010**	**01-Jan-2010**
14-Jan-2011	**31-Dec-2010**	**01-Nov-2010**	**01-Jul-2010**	**01-Jan-2009**
13-Jan-2011	**24-Dec-2010**		**01-Apr-2010**	**01-Jan-2008**
12-Jan-2011				**01-Jan-2007**
11-Jan-2011				**01-Jan-2006**
10-Jan-2011				**01-Jan-2005**

If the option [Remove retention files for overlap policy] is enabled, the overlapping snapshots would be removed, with the following snapshots available:

Daily	Weekly	Monthly	Quarterly	Yearly
16-Jan-2011	**14-Jan-2011**	~~**01-Jan-2011**~~	~~**01-Jan-2011**~~	**01-Jan-2011**
15-Jan-2011	**07-Jan-2011**	~~**01-Dec-2010**~~	~~**01-Oct-2010**~~	**01-Jan-2010**
~~**14-Jan-2010**~~	~~**31-Dec-2010**~~	~~**01-Nov-2010**~~	~~**01-Jul-2010**~~	**01-Jan-2009**
~~**13-Jan-2010**~~	~~**24-Dec-2010**~~		~~**01-Apr-2010**~~	**01-Jan-2008**
~~**12-Jan-2010**~~				**01-Jan-2007**
~~**11-Jan-2010**~~				**01-Jan-2006**
~~**10-Jan-2010**~~				**01-Jan-2005**

The weekly policy overrides the daily policy so the snapshots of 10-Jan-2011, 11-Jan-2011, 12-Jan-2011, 13-Jan-2011 and 14-Jan-2011 are removed.

The monthly policy overrides the weekly policy so the snapshots of 24-Dec-2010 and 31-Dec-2010 are removed.

The same applies to the monthly, quarterly and yearly policy giving a total of 11 snapshots.

Important:
The Retention Policy and Delta Merge feature is closely related, as the criteria for file merging is governed by the retention policy setting configured for a backup set.

Please refer to the Delta Merge section in this guide for further details.

6.1.9 Backup Filter

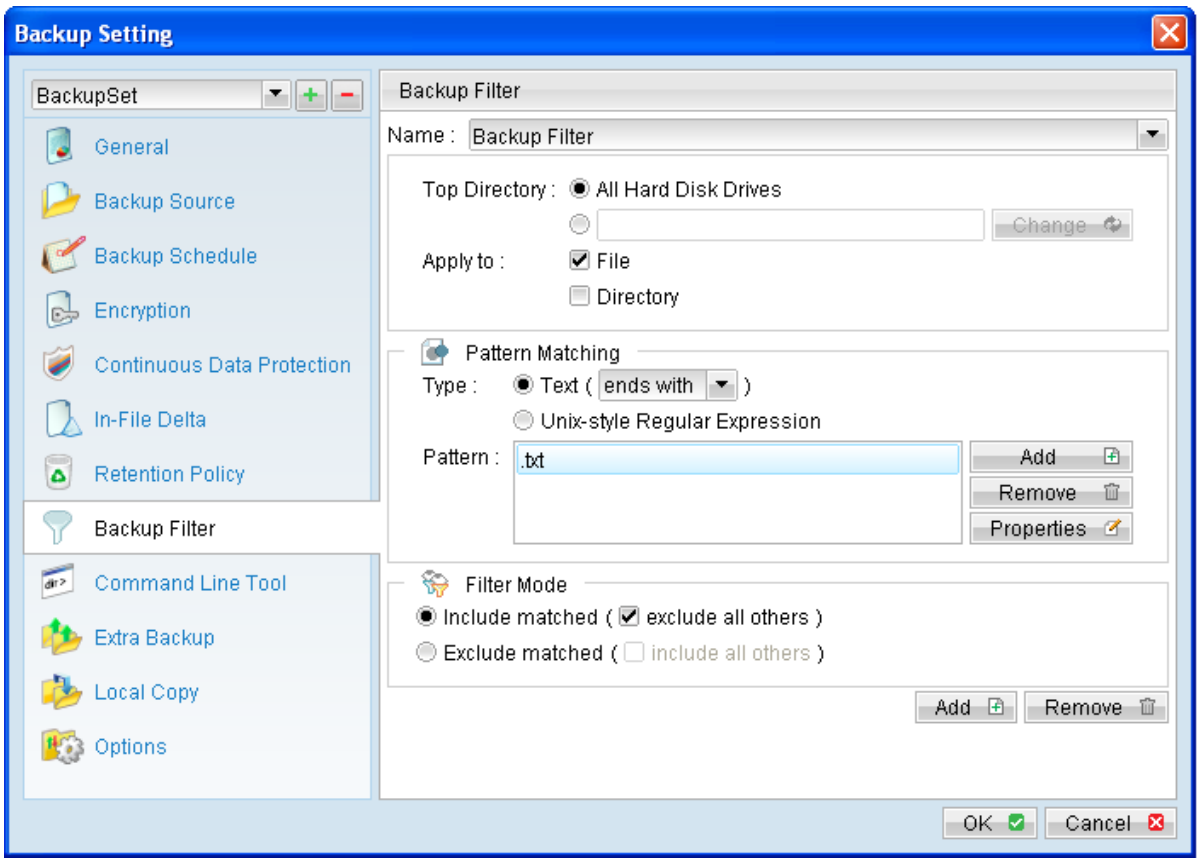
Backup Filter is a set of user defined criteria to include or exclude directories and files as backup source of a backup set.

There are some basic rules regarding backup filters:

1. Filters are applied in creation order.

2. Inclusion or exclusion made by filter takes precedence over backup source selections.

To add a new filter, press the [Add] button at the bottom of the right panel.



Menu Item	Description
Name	**The name of a filter.**
Top Directory	**The top directory to which this filter is applied. Filtering rules will be applied to all files and/or directories under this directory.** **All Hard Disk Drives – select all local hard drives as the top directory automatically.**
Apply To	**Define whether to apply the filtering rule to files and/or directories.**
Pattern Matching	**It defines the filtering rules of a filter. A filtering rule can be one of the following types;** **[Starts With]** **Include/Exclude all files/directories with name starting with a certain pattern.** **Example:** **You can use B* to match all file with name starting with a B character.** **[Contains]**

	Include/Exclude all files/directories with name containing a certain pattern. **Example:** **You can use *B* to match all files with name containing with a B character.** **[Ends With]** **Include / Exclude all files / directories with name ending with a certain pattern.** **e.g. You can use *.doc to match all files with name ending with .doc (all Word Documents)** **[Regular Expression]** **Include/Exclude all files/directories with name matching a regular expression.** **To add a new pattern, press the [Add] button in the [Pattern Matching] area.** **Note: Backup filter is case sensitive.**
Filter Mode	**Defines whether you want to include or exclude matched files into/from the backup set. Also, for those unmatched files, you can choose to exclude (if include filter type) or include (if exclude filter type) them into/from the backup set.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

The following are a list of examples with different filter settings.

Example 1:
To backup only Word, Excel and PowerPoint documents in the document directory (e.g. C:\My Documents), setup the backup filter as follows:

Top Directory = C:\My Documents
Apply To = File (true)
Matching Type = End With
Matching Patterns = *.doc, *.xls, *.ppt
Filter Mode = Include
Exclude all others = True

Example 2:
To backup all files, excluding all *.exe, *.dll and *.tmp, in C:\Application, setup the backup filter as follows.

Top Directory = C:\Applicaitons
Apply To = File (true)
Matching Type = End With

Matching Patterns = *.exe, *.dll, *.tmp
Filter Mode = Exclude
Include all others = True

Example 3:
If C:\ was selected as backup source, to exclude all images (e.g. *.jpg and *.gif) from the backup source selection, setup the backup filter as follows.

Top Directory = C:\
Apply to = File (true)
Matching Type = End With
Matching Patterns = *.jpg, *.gif
Filter Mode = Exclude
Include all others = false

Note that the [Include all others] setting is not enabled because it is not necessary to include all other file types under C:\ into the backup set.

Example 4:
To include everything, except the log directory, under C:\Applications, setup the backup filter as follows.

Top Directory = C:\Applications
Apply To = Directory (true)
Matching Type = Regular Expression
Matching Patterns = ^log$
Filter Mode = Exclude
Include all others = True

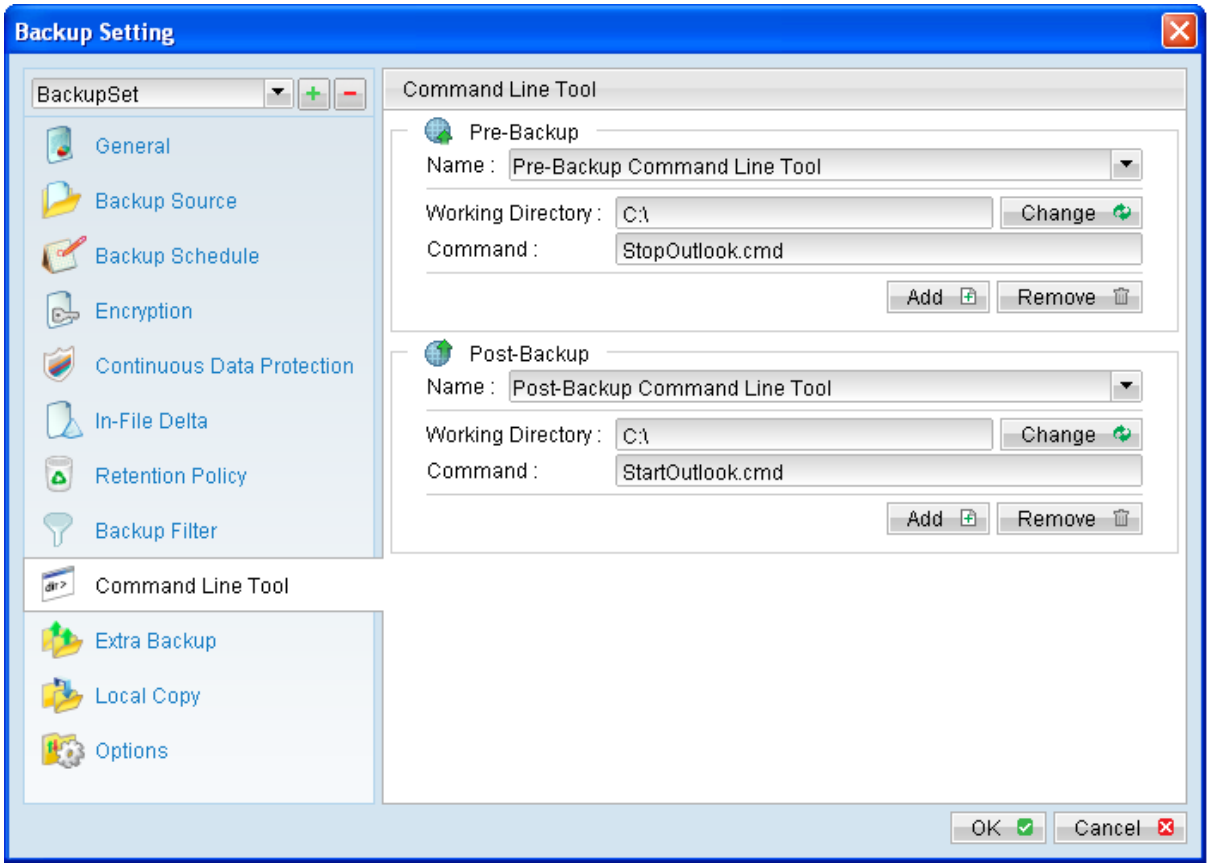
Example 5:
To include all directories named log from the backup set files with file name starting with B and ending with *.doc under C:\My Documents, the filter backup can be setup as follows.

Top Directory = C:\My Documents
Apply To = File (true)
Matching Type = Regular Expression
Matching Patterns = ^B.*\.doc$
Filter Mode = Include
Exclude all others = True

6.1.10 Command Line Tool

Click on the [Command Line Tool] tab to configure a Pre-Backup or Post-Backup command.

Command to execute batch file to stop and start an application before and after a backup job, or other command to shutdown the computer when a backup job is complete can be configured.

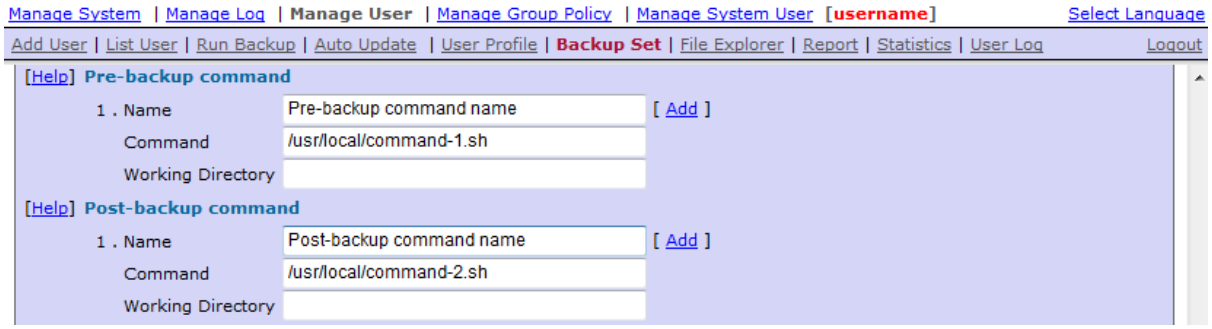


Menu Item	Description
Add	**Click to add new pre or post backup command.**
Remove	**Click to remove existing pre or post backup command.**
Name	**Input box to enter name of a pre or post backup command.**
Working Directory	**Directory which the pre or post backup command will run at.**
Command	**Input box to enter pre or post backup command to be run.** **<u>For Windows:</u>** **Native command or command to execute a batch, command or VBScript file can be configured:** **shutdown -s -t 60** **batch.bat** **command.cmd**

	script.vbs **<u>For Linux:</u>** **Command to execute a script file must be configured:** **/usr/local/command.sh** **<u>For FreeBSD / Solaris:</u>** **Command to execute a script file must be configured:** **./usr/local/command.sh** **Note:** **For all platforms, please ensure that control is returned to the backup application once the command is executed.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

For OBM installation on Linux / FreeBSD / Solaris platform (without GUI environment installed), you can setup the pre and post backup command on the web console:


Manage System | Manage Log | Manage User | Manage Group Policy | Manage System User [username] Select Language
Add User | List User | Run Backup | Auto Update | User Profile | Backup Set | File Explorer | Report | Statistics | User Log Logout
[Help] Pre-backup command
1 . Name
Pre-backup command name
[Add]
Command
/usr/local/command-1.sh
Working Directory
[Help] Post-backup command
1 . Name
Post-backup command name
[Add]
Command
/usr/local/command-2.sh
Working Directory

Menu Item	Description
Add	**Click to add new pre or post backup command.**
Remove	**Click to remove existing pre or post backup command.**
Name	**Input box to enter name of a pre or post backup command.**
Command	**Input box to enter pre or post backup command to be run.** **Pre and post command must be put into a**

	script file. It is also recommended to add the absolute path location of the script, such as: **/pathname/scriptname.sh** **Note:** **Please ensure that control is returned to the backup application once the command is executed.**
Working Directory	**Location the script would be working from.** **This field can be left empty, but please note that any output from the script would be stored under the OBM installation folder.**
Update	**Click to save the changes.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

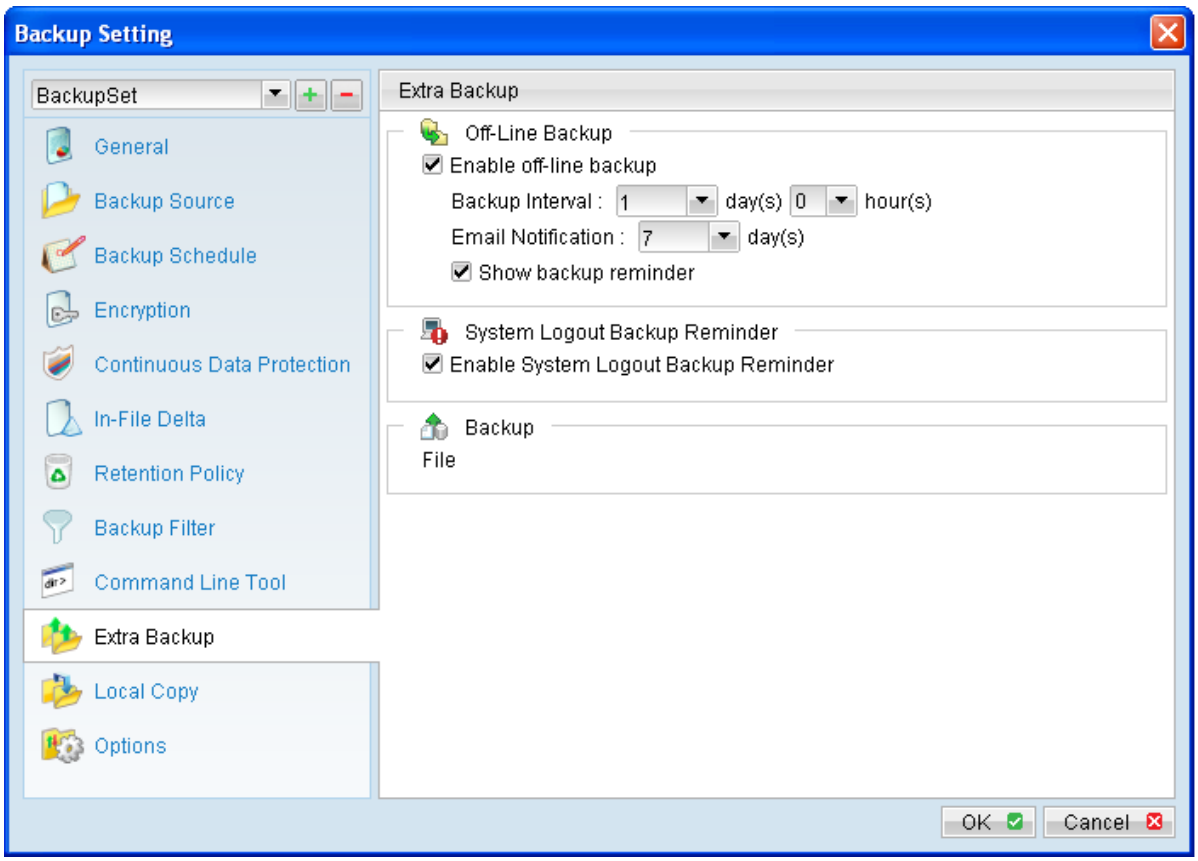
The pre and post backup command will run at different stages of a backup according to it backup type.

The following table outlines when they would be run:

Backup type	Pre-Backup command	Post-Backup command
File backup type	**Run before any file is backed up (uploaded) to the backup server.**	**Run when the backup (upload) of all files are completed.**
Non-file backup type	**Run before any database file is spooled to the designated temporary directory.**	**Run after spooling backup files to temporary directory (e.g. before the first backup file is uploaded).**

6.1.11 Extra Backup

Click on the [Extra Backup] tab to enable the Off-Line Backup and System Logout Backup Reminder option.



Note:
[Extra Backup] tab is only available for OBM installation on Windows platforms.

6.1.1.11 Enable off-line backup

Enable off-line backup defines whether to enable the [off-line backup] feature.

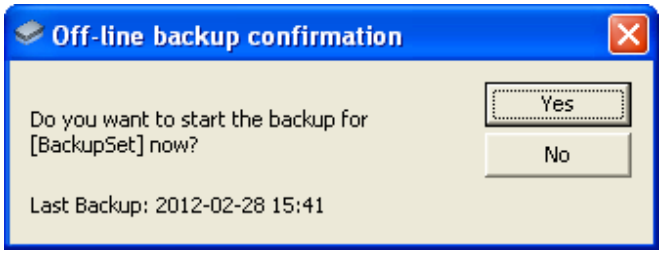
The [off-line backup] feature is designed for notebook users who may be off-line most of the time, and cannot rely on backup scheduled for regular backup of their data.

Enable off-line backup	Action
Enabled	Prompt for backup if the time between the last backup to the current time exceeded the [Backup Interval].
Disabled	Do not prompt for backup.
Backup Interval	Time interval between each backup job.
Email Notification	Time interval when email would be sent for backup reminder.
Show backup reminder	To display or hide the confirmation dialog for

	backup. If the confirmation dialog is disabled, backup will be performed automatically when connection to the Internet is re-established.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

With the [off-line backup] setting is enabled, when the computer is connected online and the time between the last backup to the current time elapsed the [Backup Interval], a pop up off-line backup confirmation menu will be prompted, reminding the user to perform a backup.



Menu Items	Description
Yes	Perform the backup job immediately.
No	Do not perform the backup job.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

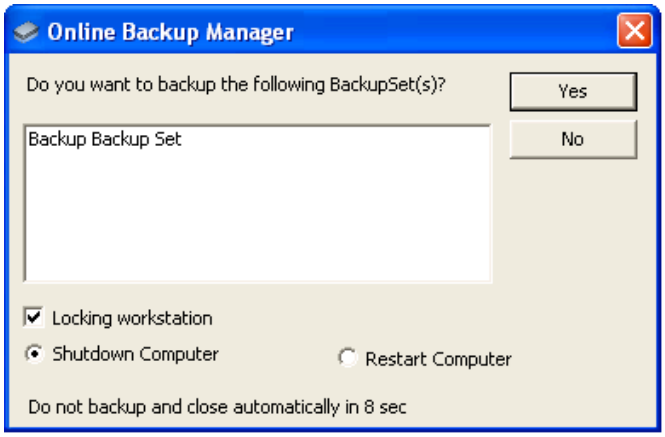
6.1.2.11 Enable System Logout Backup Reminder

Enable System Logout Backup Reminder defines whether to enable the [System Logout Backup Reminder] feature.

Enable System Logout Backup Reminder	Action
Enabled	Prompt for backup before logging out or shutting down.
Disabled	Do not prompt for backup.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

When the [System Logout Backup Reminder] setting is enabled, a pop up logout reminder menu will be prompted, requesting for backup before the user logs out of the system or before shutting down Windows.



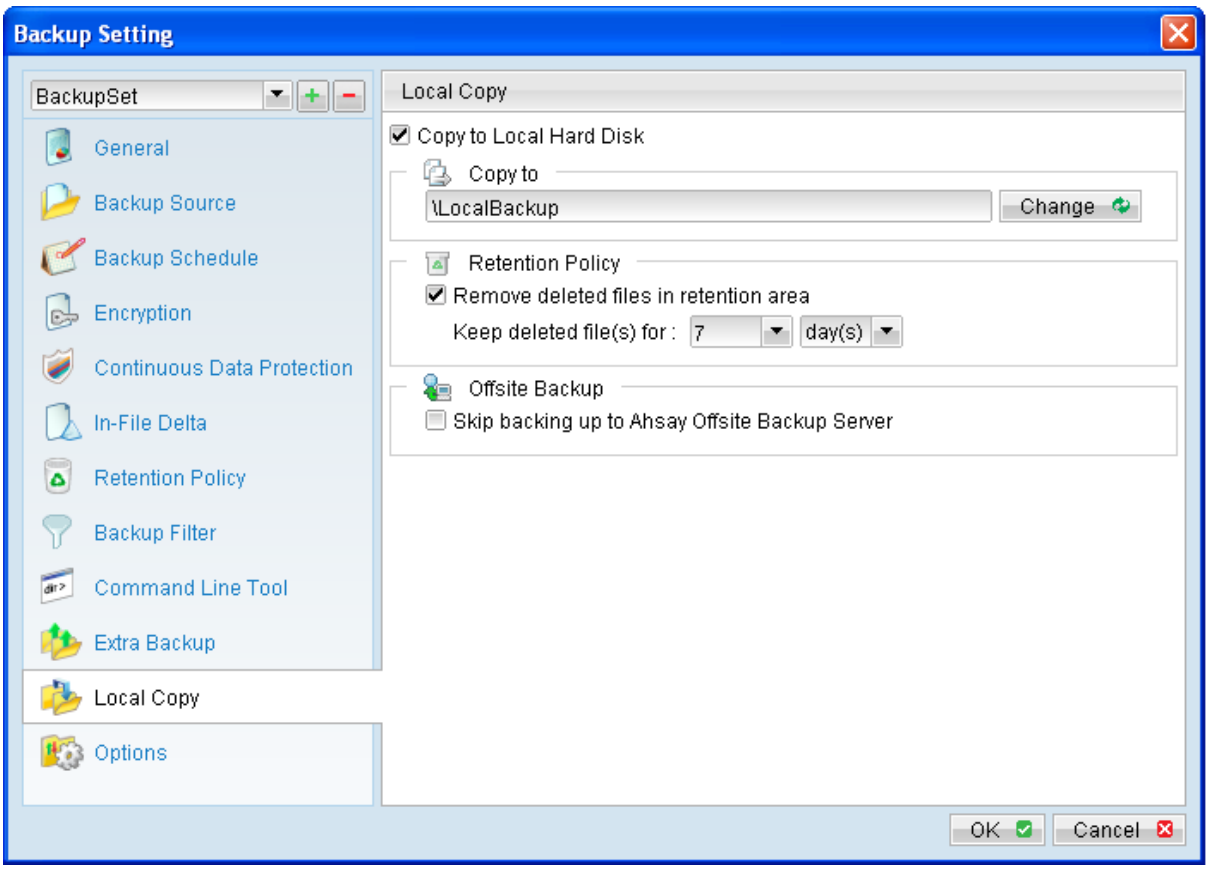
Menu Items	Description
Yes	Click to perform a backup for the backup set before logging out or shutting down.
No	Click to proceed to logout or shutdown directly.
Locking workstation	Checkbox to lock the corresponding machine when the backup is being performed.
Shutdown Computer	Radio button to shutdown computer after the backup job is completed.
Restart Computer	Radio button to restart computer after the backup job is completed.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

6.1.12 Local Copy

To save a copy of back up data locally on the client computer, simply enable the local copy feature of the backup client application.

Click on the [Local Copy] tab to configure a local copy backup.



Menu Items	Description
Copy to Local Hard Disk	Checkbox to enable or disable local copy backup.
Copy to	Directory which the local copy data are stored.
Remove deleted files in retention area	Checkbox to enable or disable the retention policy of the local copy backup.
Keep deleted file(s) for	Dropdown menu to select a basic retention policy. Note: For local copy backup, only basic retention policy can be applied.
Skip backing up to Offsite Backup Server	Checkbox to skip or to perform off-site backup for the corresponding backup set.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Select the corresponding backup set from the drop down menu, and click on the [Local Copy] tab.

Select the checkbox beside [Copy to Local Hard Disk], click the [Change] button and browse to the directory path which you would like to store the local copy backup.

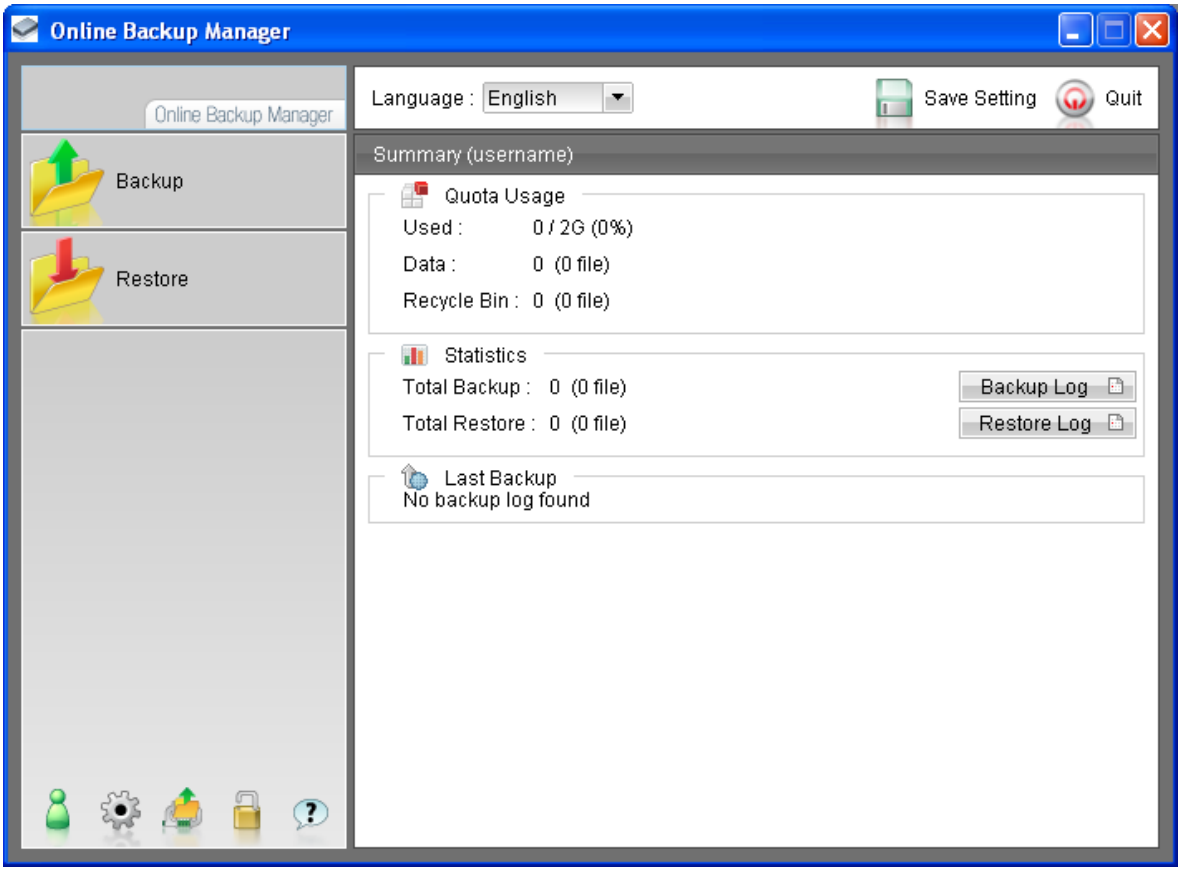
You can enable retention policy for the local copy backup (if necessary). However, note that only basic retention policy can be configured for local copy.

Retention policy of the local copy backup is separate from the retention policy configured for the off-site backup (configured in the [Retention Policy] tab).

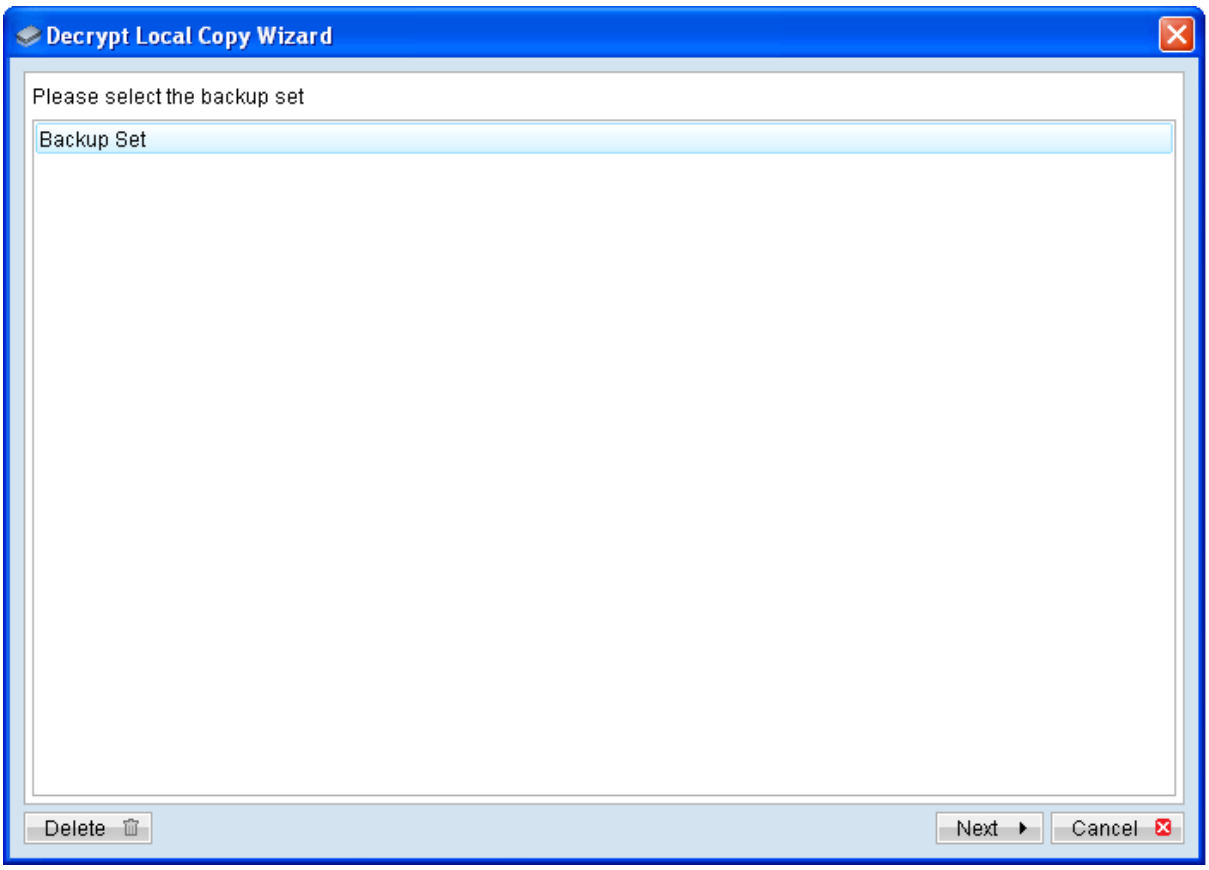
For backup set that is intended for local copy backup only, select the checkbox beside [Skip backing up to Offsite Backup Server].

Data that are backed up by the local copy module are compressed and encrypted. To restore local copy backed up files, please refer to the following instruction:

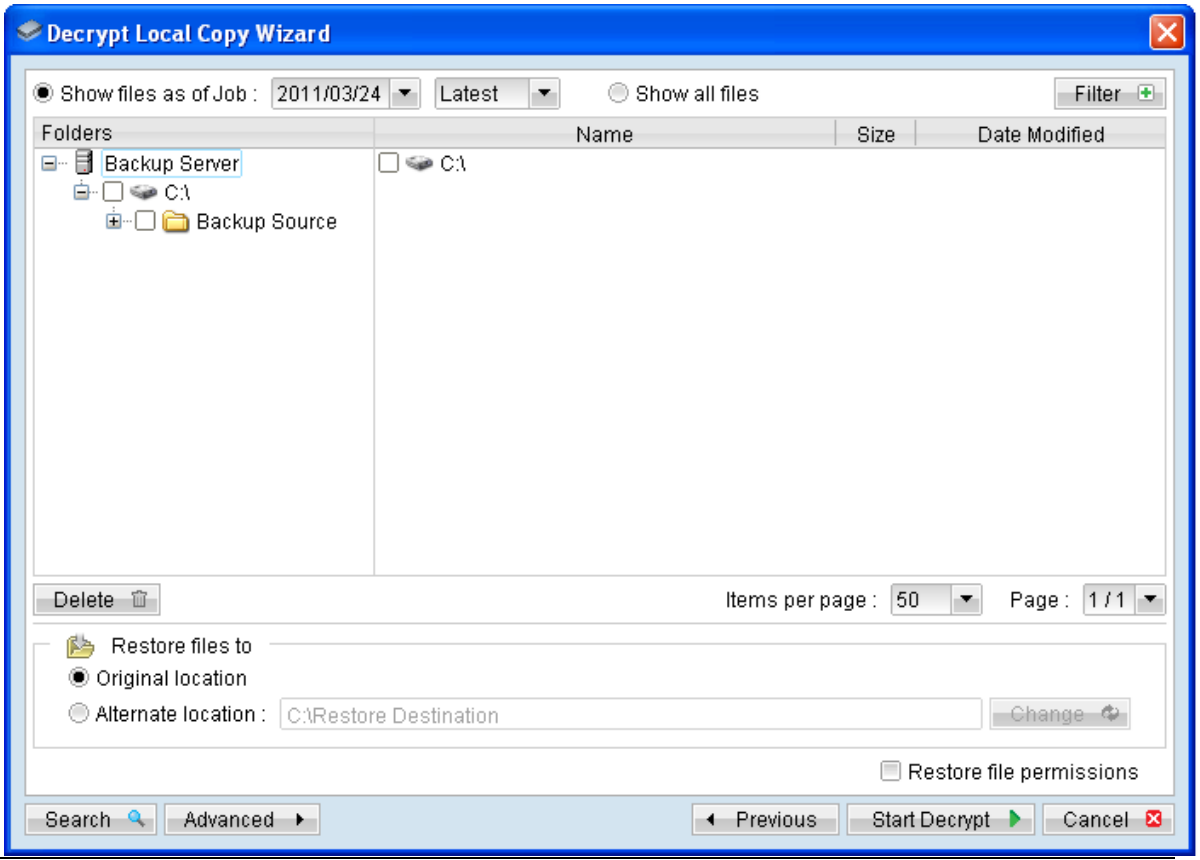
1. Press the [Decrypt Local Copy Wizard] button on the backup application's main window.



2. Select the backup set to be restored and press [Next] to proceed.



3. Follow the normal restore procedure for restoration of your local copy backed up data. For more details, please refer to Chapter 8 of this guide.

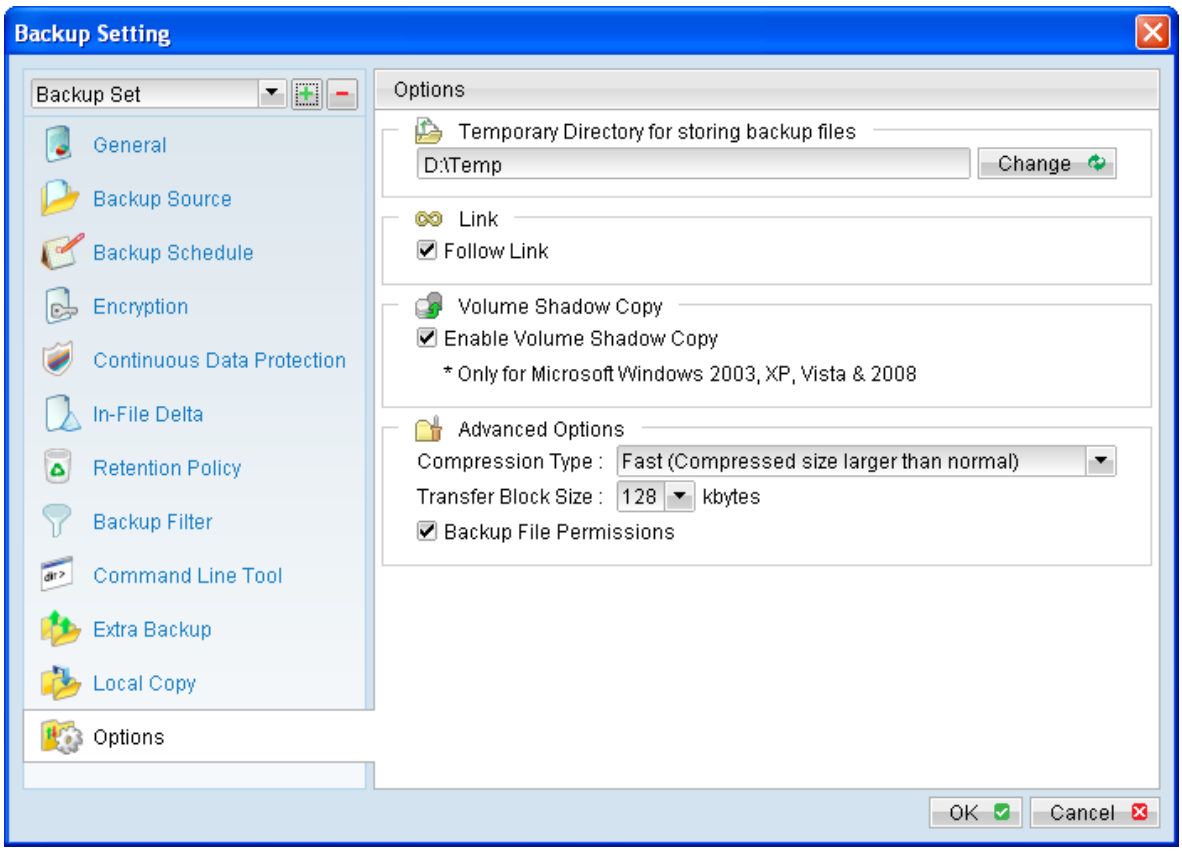


6.1.13 Options

Click on the [Options] tab to configure options such as temporary directory for storing backup files, follow link, Volume Shadow Copy or advance option such as the transfer block size.

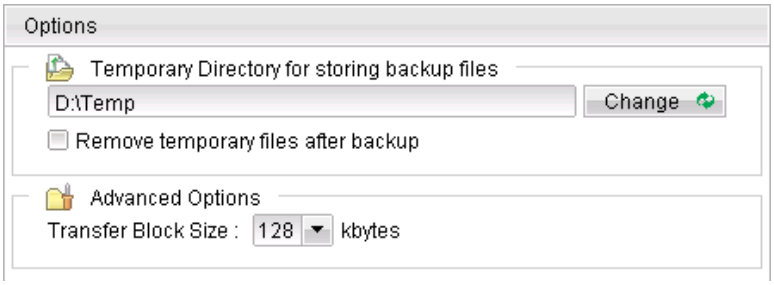
6.1.1.13 Temporary Directory for storing backup files

The temporary directory is used for various purposes, such as storage of temporary spooled file (for database specific backup type), remote file list, local file list, temporary delta file and other files of temporary nature.



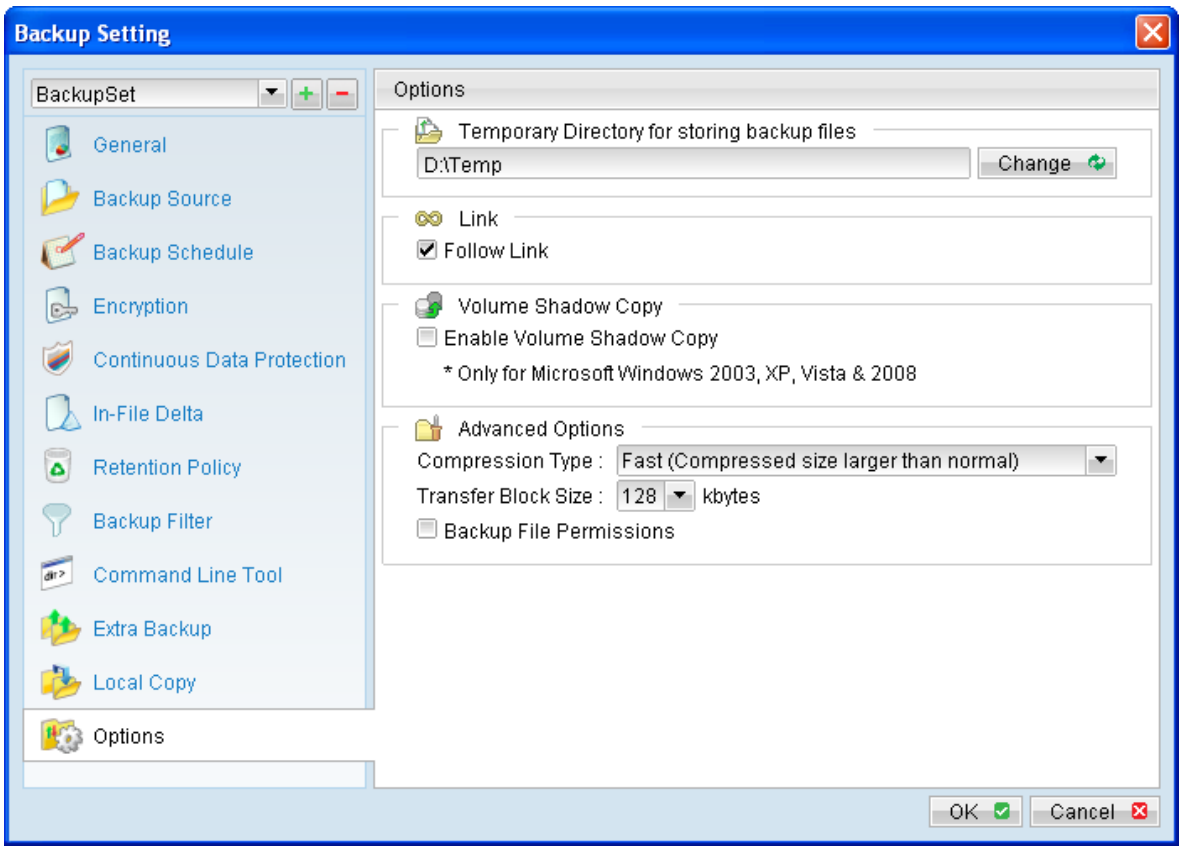
To configure the temporary directory location, click [Change] and browse to the directory path for storing the temporary data.

For database specific backup type, data files spooled by the **latest backup job** can be kept by disabling the [Remove temporary files after backup] option.



6.1.2.13 Follow Link

Follow Link defines whether to follow an NTFS junction point or NTFS symbolic link during backup.



Follow Link	Action
Enabled	Backup junction point or symbolic link as well as the directories and files that it links to (even if the target data are not located under the backup source).
Disabled	Backup junction point or symbolic link only.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

When the follow link option is enabled, not only is the symbolic link or junction point backed up, but directories and files that the junction point links to will also be backed up.

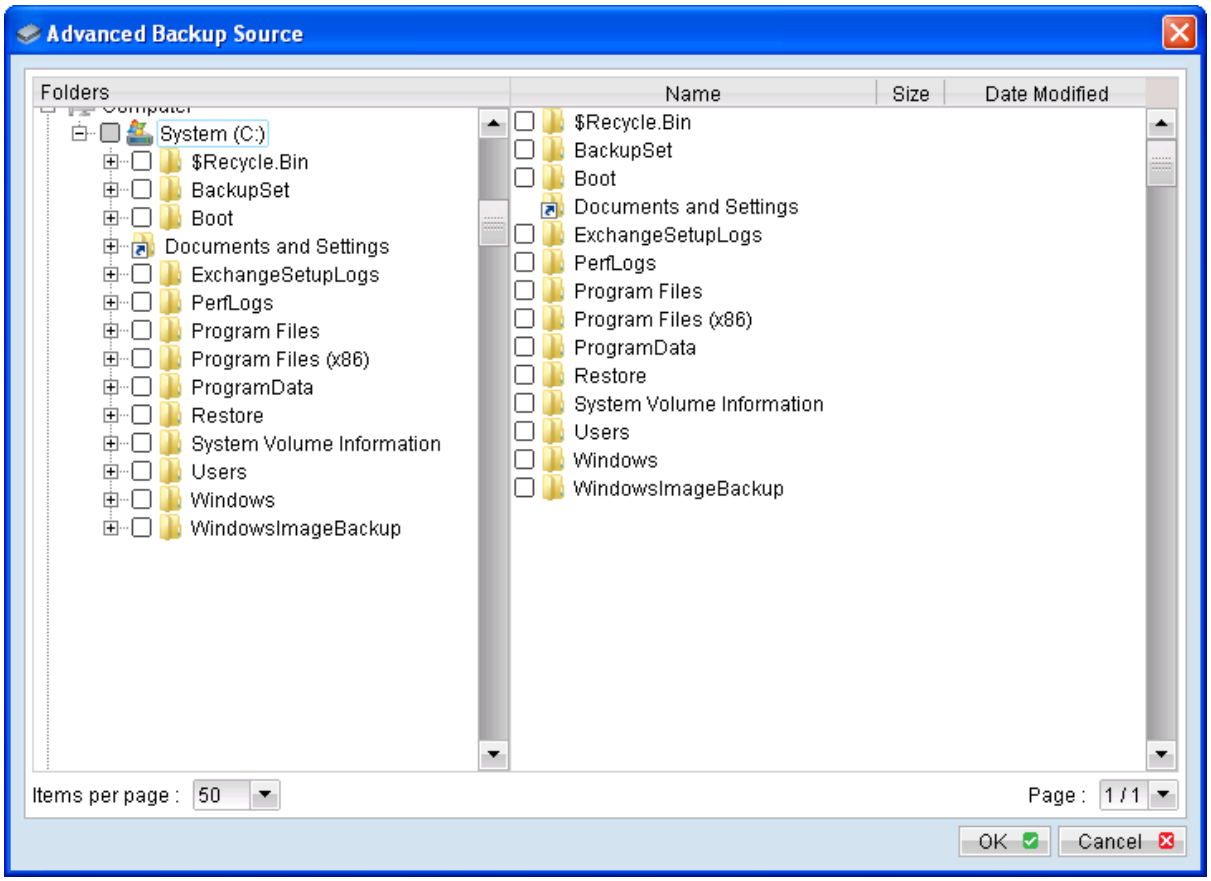
Restore outcome would be different with the different setting used during backup and restore (e.g. there is a follow link option for backup and a follow link option in the restore menu).

The following table summarizes the outcome when a restore is performed with different options:

Follow Link	Restore to	Action
Enabled	Original Location	Junction points are restored to the original location. Restore follow link option enabled - Target directories and files are restored to the original location. Restore follow link option disabled - Target directories and files are not restored.
	Alternate Location	Junction points are restored to the location specified. Restore follow link option enabled - Target directories and files are restored to the location specified. Restore follow link option disabled - Target directories and files are not restored.
Disabled	Original Location	Junction points are restored to the original location. No data is restored to the junction point's destination.
	Alternate Location	Junction points are restored to the location specified. No data is restored to the junction point's destination.

To enable the [Follow Link] option, select the checkbox beside the follow link option.

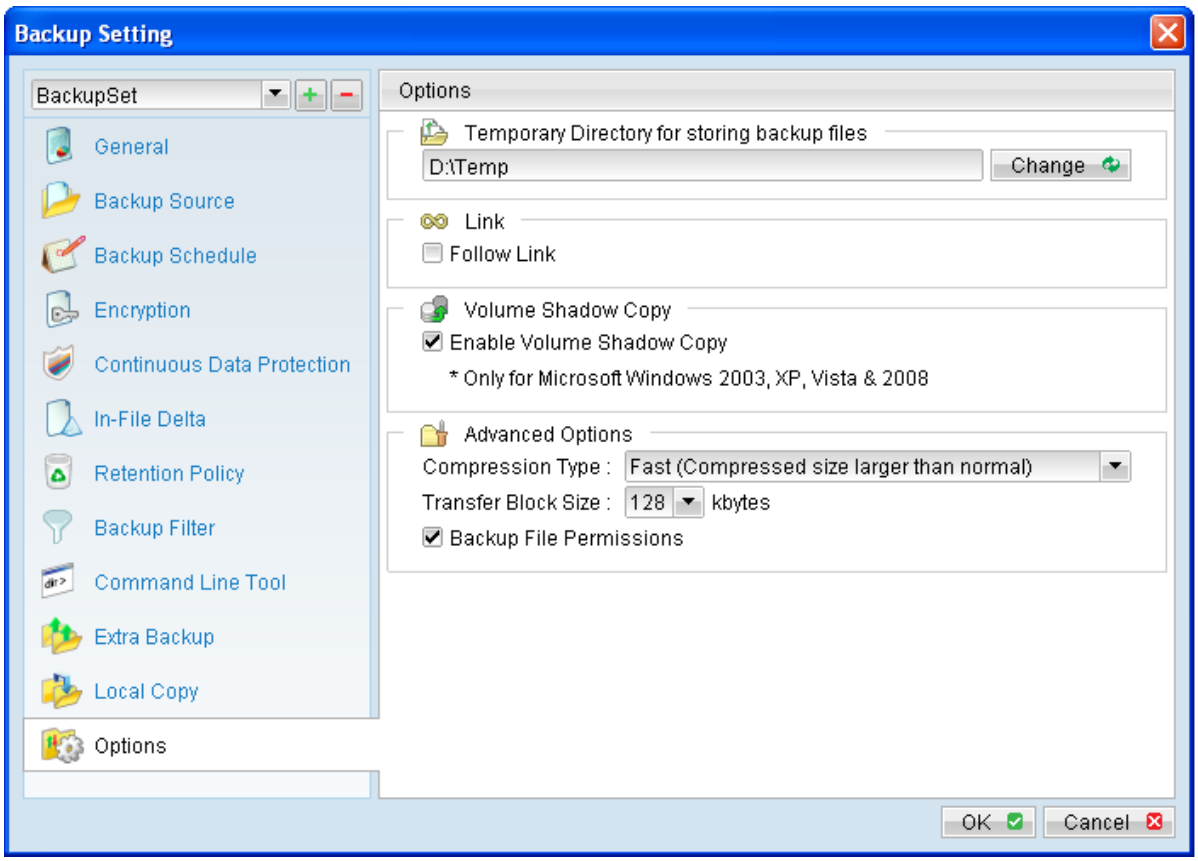
Note that system protected junction point such as the Documents and Settings on Windows 2008 server cannot be selected as backup source under the advanced backup source dialog (e.g. there is no select-able checkbox beside system protected junction point).



To manually select system protected junction points for backup, select the parent directory of the junction point, or enter the corresponding junction point (e.g. C:\Documents and Settings) on the web interface.

6.1.3.13 Enable Volume Shadow Copy

Enable Volume Shadow Copy defines whether to enable Microsoft Volume Shadow Copy Service (VSS) for the backup set.



Enable Volume Shadow Copy	Action
Enabled	Create a snapshot of the data to be backed up for exclusively opened file.
Disabled	Do not create a snapshot of the data to be backed up for exclusively opened file. Error message will be shown for files that are opened during the backup process.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Enabling the Volume Shadow Copy option will allow backup of local files that are exclusively opened during the backup process (e.g. Outlook PST file).

Some requirements of the Volume Shadow Copy option include:

- Volume Shadow Copy can only be applied for local drive; exclusively opened file on network shared drive cannot be backed up even with the Volume Shadow Copy option enabled.
- Volume Shadow Copy is only available on Windows platforms released after Windows 2000 (e.g. XP / 2003 / Vista / 2008 / 7 / SBS 2011).

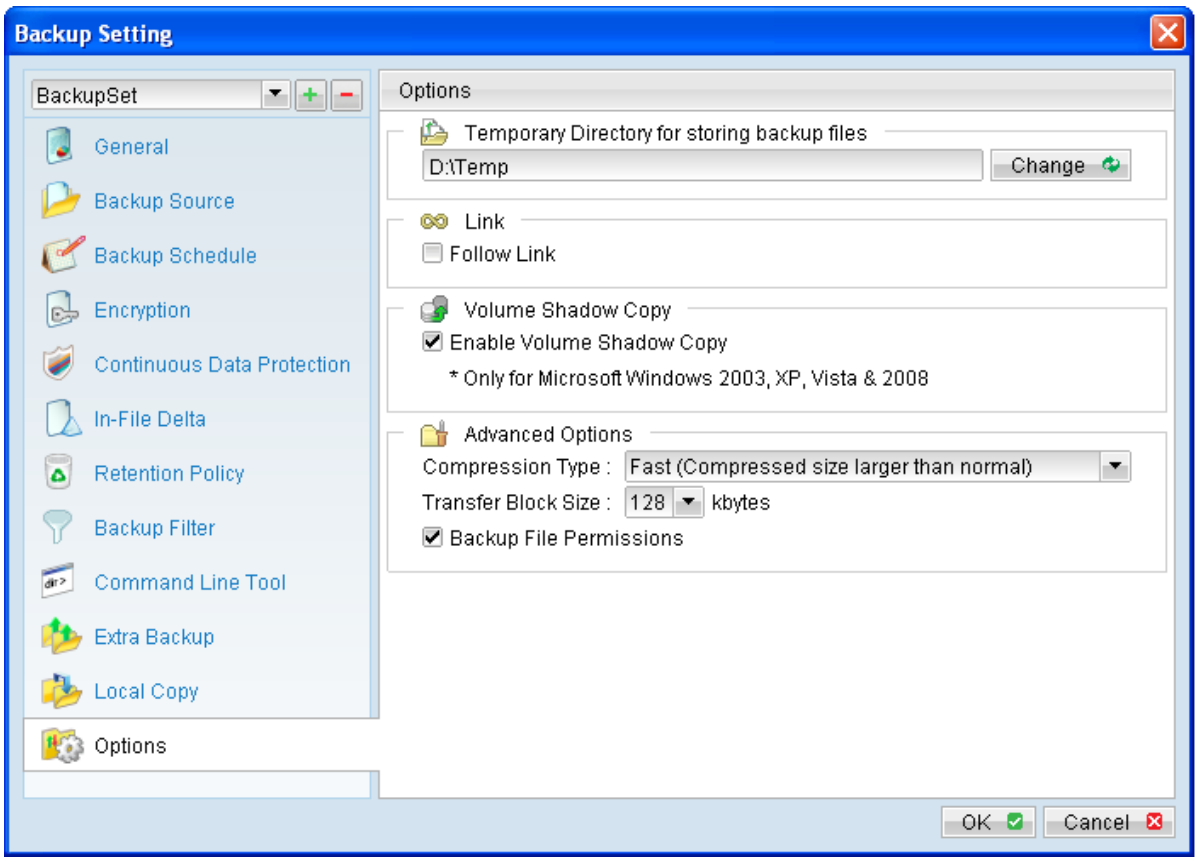
- The user using the backup application must have administrative privileges to access the Volume Shadow Copy service on a computer.
- At least one of the partitions on the machine must be in NTFS format.

For more technical information on Volume Shadow Copy, please refer to following page from Microsoft for details:

http://technet.microsoft.com/en-us/library/cc785914(WS.10).aspx

6.1.4.13 Compression

Compression type defines the compression method that the backup application will use during backup (for the corresponding backup set).



There are 3 compression types available for user to select:

- No Compression
- Normal
- Fast (Compressed size larger than normal)

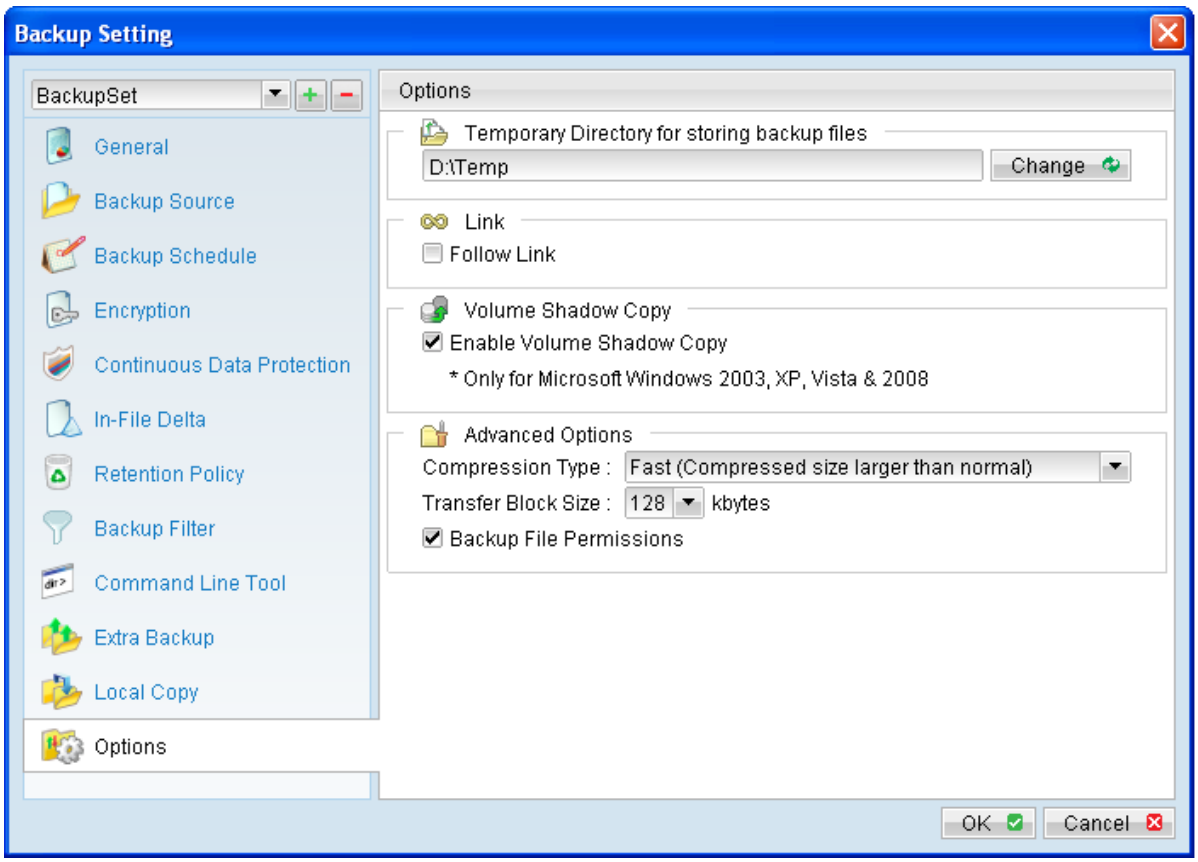
By default, newly created backup set is configured to uses [Fast] compression type.

Note:
The [Compression Type] option is only available for OBM version 6.9 or above connecting to backup server version 6.9 or above (please consults your service provider for details).

For existing backup set created in previous version, the compression type will be [Normal].

6.1.5.13 Transfer Block Size

Transfer block size defines the block size that the backup application will use to transfer your backup data to the backup server.



Note that certain firewall applications or proxy servers may block out-going network traffic with large block size for security reasons. If you are in a network with this type of restriction, please lower the transfer block size value.

To change the transfer block size of any backup set, select the [Options] tab on the left panel and then select the corresponding block size from the [Transfer Block Size] dropdown menu.

Press the [OK] button, and save before exiting out of the backup application.

6.1.6.13 Backup File Permission

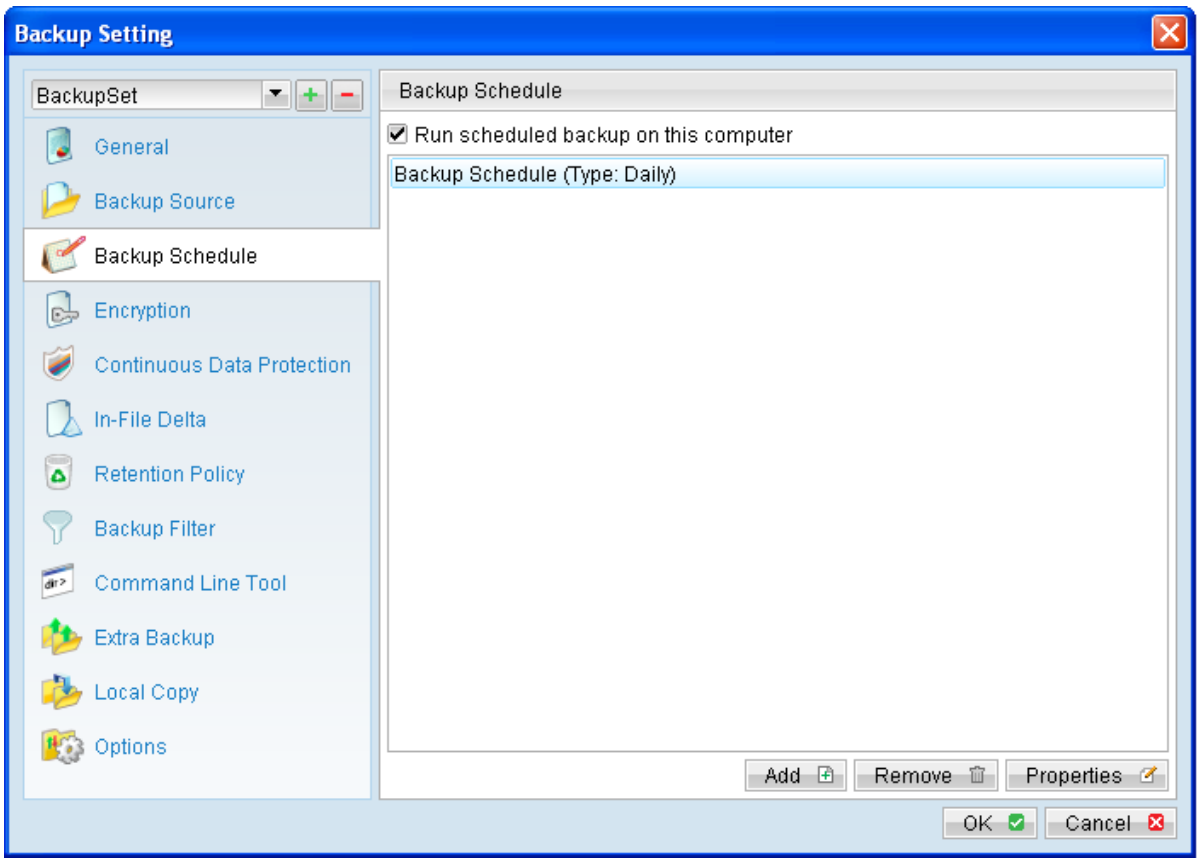
Backup file permission defines whether to backup operating system file permission of the data selected as backup source.

6.2 Single backup account for multiple computers

Multiple client computers can be backed up with a single backup user account. However, **separate backup set** must be created for **each computer**, because backup set cannot be shared.

To setup a single backup account for 10 client computers, 10 backup sets must be created, with specific backup set for each computer.

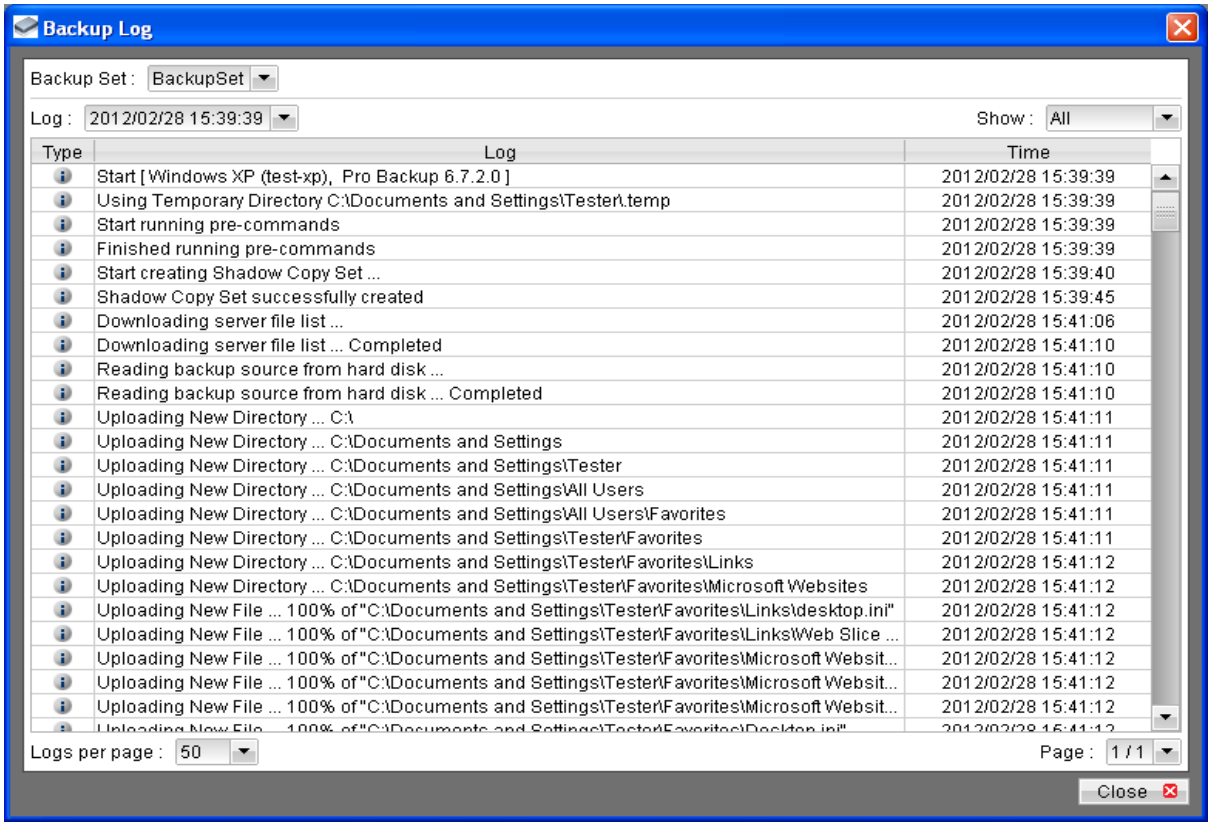
When creating backup sets in this environment, please ensure that the [Run scheduled backup on this computer] setting is properly configured for each computer. Failure to do so may result in data lost.



7 File Backup

This chapter describes in details how to perform a file backup with OBM.

7.1 File backup process


Backup Log
Backup Set : BackupSet
Log : 2012/02/28 15:39:39
Show : All
Type
Log
Time
Start [Windows XP (test-xp), Pro Backup 6.7.2.0] 2012/02/28 15:39:39
Using Temporary Directory C:\Documents and Settings\Tester\.temp 2012/02/28 15:39:39
Start running pre-commands 2012/02/28 15:39:39
Finished running pre-commands 2012/02/28 15:39:39
Start creating Shadow Copy Set ... 2012/02/28 15:39:40
Shadow Copy Set successfully created 2012/02/28 15:39:45
Downloading server file list ... 2012/02/28 15:41:06
Downloading server file list ... Completed 2012/02/28 15:41:10
Reading backup source from hard disk ... 2012/02/28 15:41:10
Reading backup source from hard disk ... Completed 2012/02/28 15:41:10
Uploading New Directory ... C:\ 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings\Tester 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings\All Users 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings\All Users\Favorites 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings\Tester\Favorites 2012/02/28 15:41:11
Uploading New Directory ... C:\Documents and Settings\Tester\Favorites\Links 2012/02/28 15:41:12
Uploading New Directory ... C:\Documents and Settings\Tester\Favorites\Microsoft Websites 2012/02/28 15:41:12
Uploading New File ... 100% of "C:\Documents and Settings\Tester\Favorites\Links\desktop.ini" 2012/02/28 15:41:12
Uploading New File ... 100% of "C:\Documents and Settings\Tester\Favorites\Links\Web Slice ... 2012/02/28 15:41:12
Uploading New File ... 100% of "C:\Documents and Settings\Tester\Favorites\Microsoft Websit... 2012/02/28 15:41:12
Uploading New File ... 100% of "C:\Documents and Settings\Tester\Favorites\Microsoft Websit... 2012/02/28 15:41:12
Uploading New File ... 100% of "C:\Documents and Settings\Tester\Favorites\Microsoft Websit... 2012/02/28 15:41:12
Logs per page : 50
Page : 1 / 1
Close

Stages of a backup job are outlined below:

1. A connection from the backup client application to the backup server is established.

2. A Shadow Copy set of the backup source volume is created (if available).

3. Download the server file list from the backup server.

4. Data of the backup source is compared with the server file list to compile the following file lists:

   - New file list
   - Modified file list
   - Deleted file list

5. Delta file is generated for modified file (if necessary).

   Note:

Only modified part of a file (delta file) is uploaded to the backup server, reducing the time required to complete the backup job.

6. Data are encrypted, compressed, and then uploaded onto the backup server.

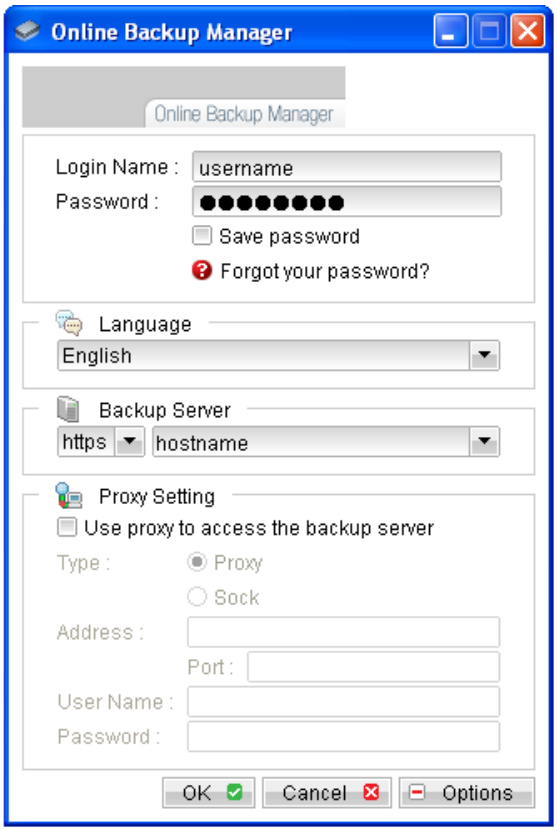
7. The Shadow Copy set of the backup source is removed (if necessary).

8. Backup is completed successful.

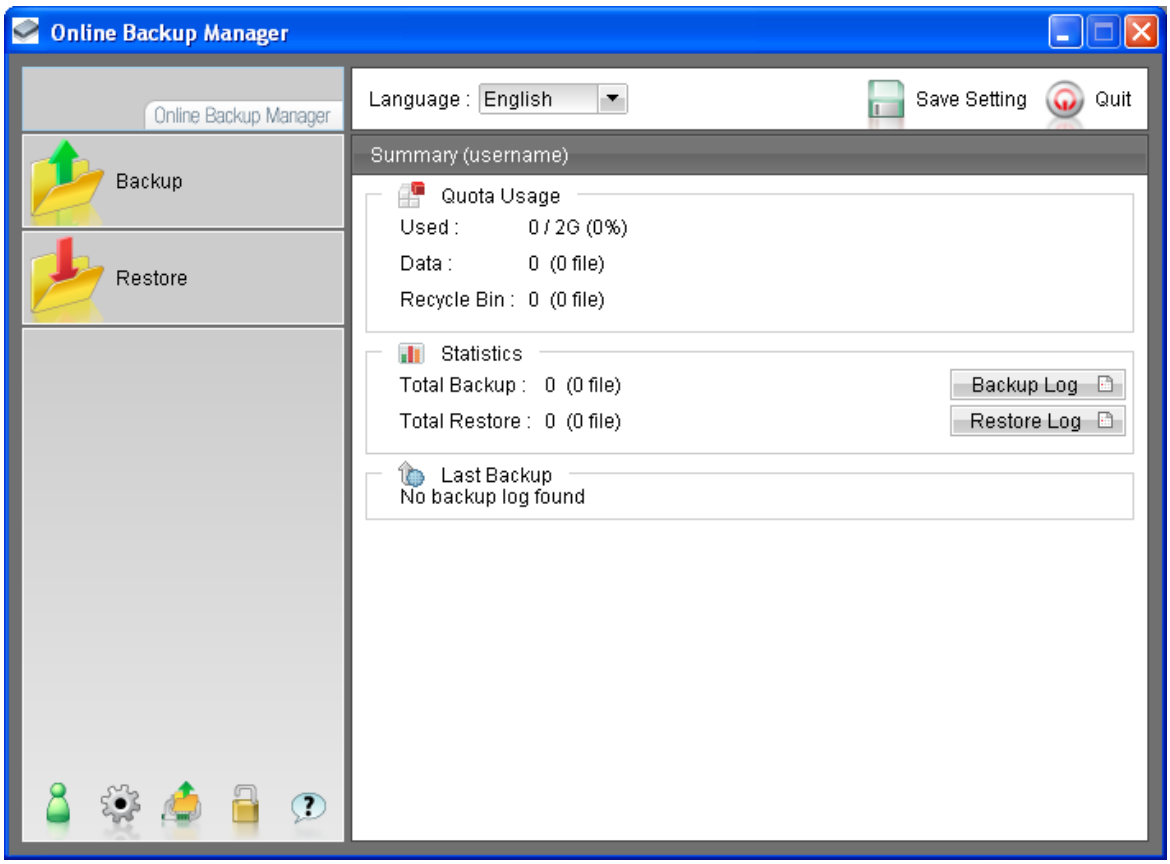
7.2 How to start an off-site backup

Please refer to the following steps for starting an off-site backup:

1. Login to the backup application's user interface.



2. Click on the [Backup] button on the backup application's main window to perform a backup manually.



3. For scheduled backup, a backup job would be automatically performed at the scheduled time specified.

   Note:
   Scheduled backup job may be missed if the client computer is switched off, in hibernated, standby mode.

   Please ensure that the computer is not in the mode stated above at the scheduled backup time.

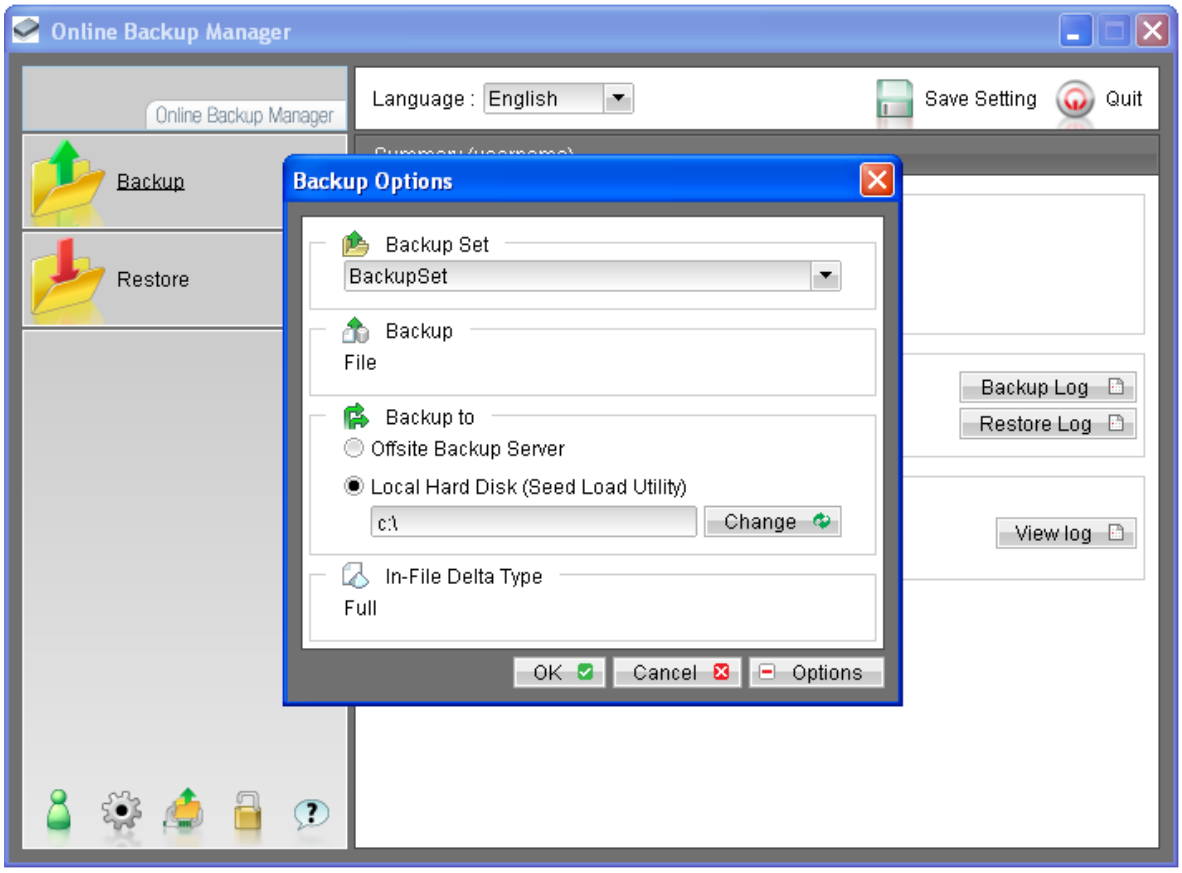
7.3 Seed Load backup

For backup of large amount of data, it would take a considerable amount of time to perform the initial full backup through the Internet.

To reduce the time and bandwidth required for initial backup, the Seed Load Utility can be utilized to perform initial backup to a local remove-able hard disk at the client site, instead of backing up through the Internet.

The backed up data can then be transported to your service provider, where they can import the data on the remove-able hard disk into your backup account on their server.

To access the Seed Load Utility, you will need to access the backup option menu:

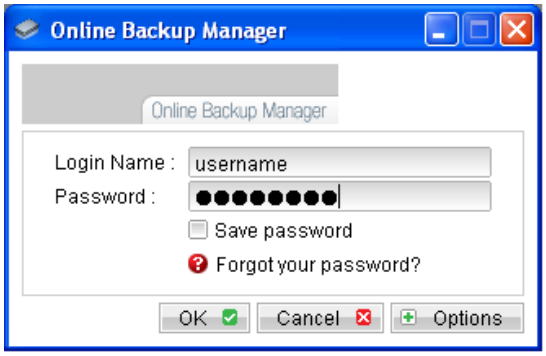


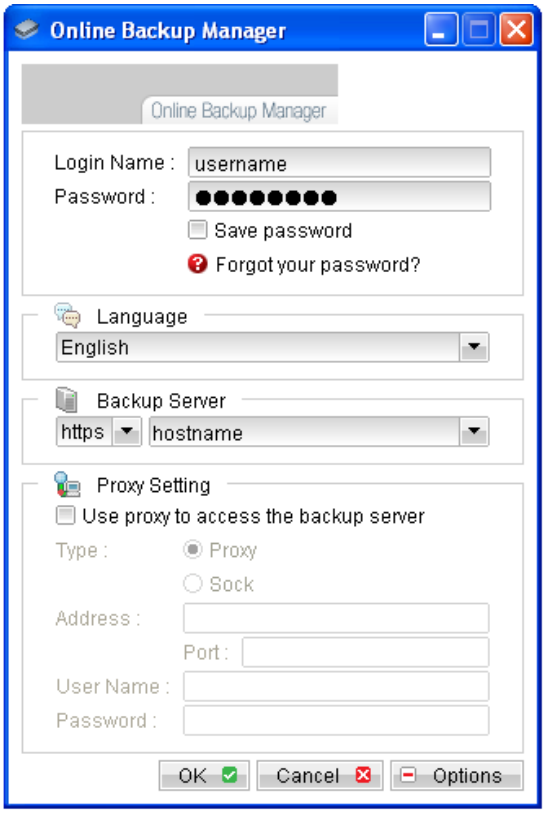
Menu Items	Description
Backup Set	Dropdown menu to select backup set.
Local Hard Disk (Local Copy)	Radio button to enable backup to local hard disk for local copy backup.
Local Hard Disk (Seed Local Utility)	Radio button to enable backup to local

	hard disk for seed load backup.
Change	Click to browse to the directory path which you would like to store the seed load backup.

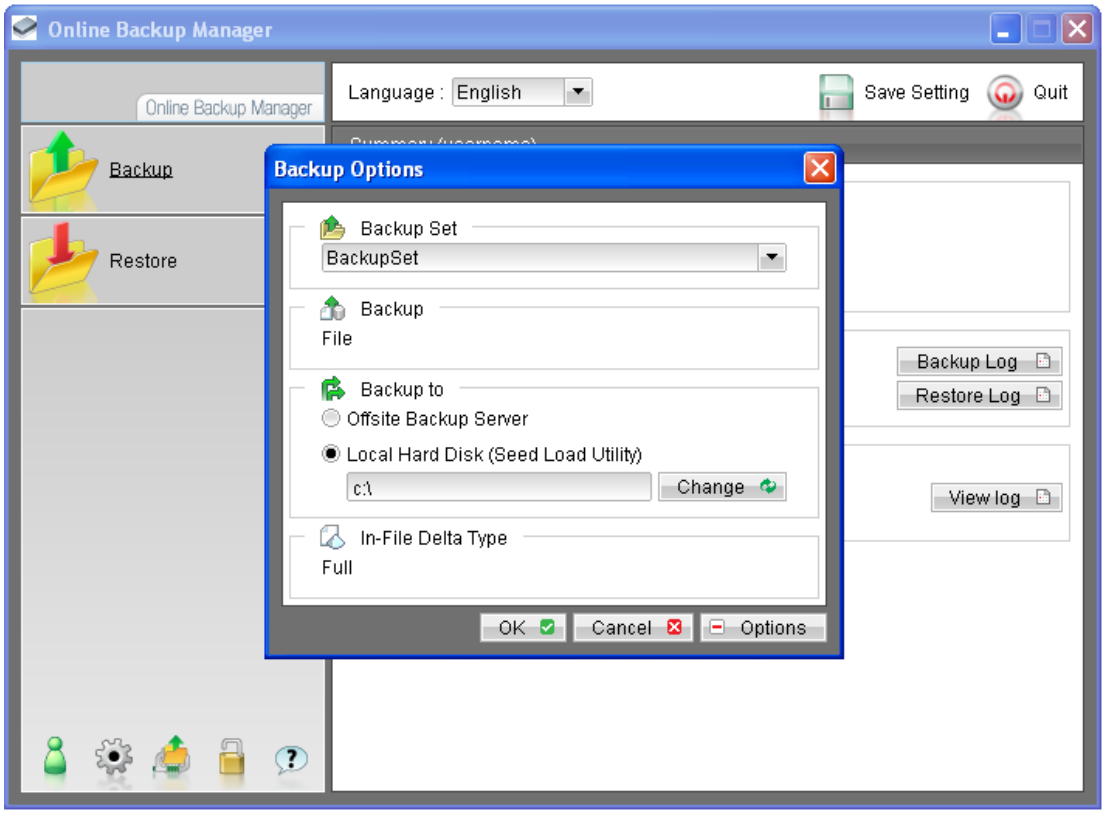
To start a seed load backup:

1. Login to the backup application's user interface.





2. Select the [Options] button to expand the backup options menu.



Menu Items	Description
Backup Set	Dropdown menu to select backup set.
Local Hard Disk (Local Copy)	Radio button to enable backup to local hard disk for local copy backup.
Local Hard Disk (Seed Local Utility)	Radio button to enable backup to local hard disk for seed load backup.
Change	Click to browse to the directory path which you would like to store the seed load backup.

3. Select the corresponding backup set.

4. Select the radio button beside [Local Hard Disk (Seed Load Utility)].

5. Click on the [Change] button to browse to the directory path which you want the seed load data to be stored at (e.g. the remove-able hard disk).

6. Press the [OK] button to start the backup job.

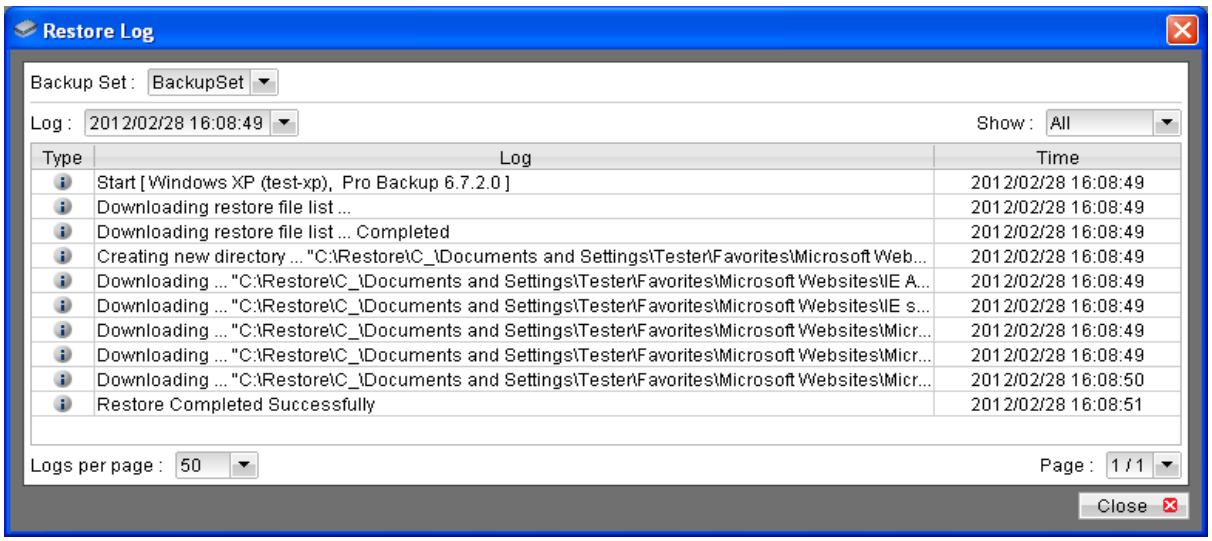
7. Transport the data in the specific directory to OBS.

Note:
A seed load backup can only be performed manually.

8 File Restore

This chapter describes in details how to perform a file restore with OBM.

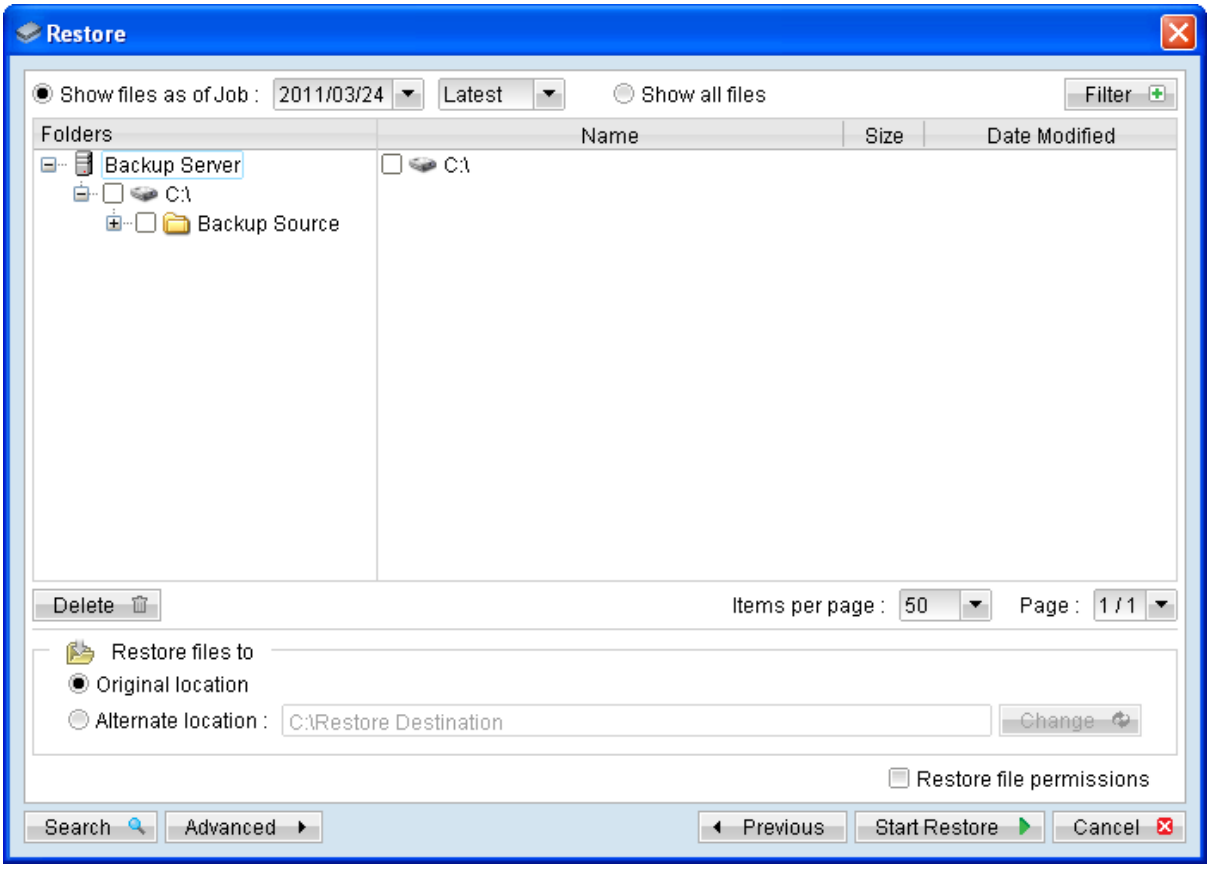
8.1 File restore process


Restore Log
Backup Set : BackupSet
Log : 2012/02/28 16:08:49
Show : All
Type
Log
Time
Start [Windows XP (test-xp), Pro Backup 6.7.2.0] 2012/02/28 16:08:49
Downloading restore file list ... 2012/02/28 16:08:49
Downloading restore file list ... Completed 2012/02/28 16:08:49
Creating new directory ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Web... 2012/02/28 16:08:49
Downloading ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Websites\IE A... 2012/02/28 16:08:49
Downloading ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Websites\IE s... 2012/02/28 16:08:49
Downloading ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Websites\Micr... 2012/02/28 16:08:49
Downloading ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Websites\Micr... 2012/02/28 16:08:49
Downloading ... "C:\Restore\C_\Documents and Settings\Tester\Favorites\Microsoft Websites\Micr... 2012/02/28 16:08:50
Restore Completed Successfully 2012/02/28 16:08:51
Logs per page : 50
Page : 1 / 1
Close

Stages of a restore are outlined below:

1. A connection from the backup client application to the backup server is established.
2. Download the restore file list from the backup server.
3. Create the directory path for the restoration (if necessary).
4. Download the backup data from the backup server.
5. All the data will be decompressed and decrypted on the backup client computer.
6. Merging of delta files (for file with multiple delta files, if necessary).
7. Merging of combined delta file with full file.
8. Restore is completed successfully.

8.1.1 Restore Menu



Menu Items	Description
Show files as of Job	Radio button to display files available for restore as of which backup job.
[YYYY/MM/DD]	Dropdown menu to select the date of a backup job (used with the [Show files as of Job] option).
[hh/mm/ss]	Dropdown menu to select the time of a backup job (used with the [Show files as of Job] option).
Show all files	Radio button to display all files available for restore.
Filter	Click to open the filter option.
Delete	Click to delete the selected file from OBS. **Important:** File will not be available for restore in the future if they are deleted from OBS.
Original location	Restore directories and files to their original location.
Alternate location	Restore directories and files to an alternate location

	specified.
Change	Click to change the directory path of the restore destination.
Restore file permissions	Checkbox to enable or disable restore of file permission.
Search	Click to open the Search option.
Advanced	Click to open advanced option: Delete extra files - Click to synchronize the selected restore source with the restore destination during the restore process. Follow Link – Click to restore link destination's data.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Select the [Show files as of Job] to display files available as of a particular backup job.

For example, to display the files available for restore since the backup job performed on 11:00am Mar 11th, 2011. Select [Show files as of Job], [2011/03/11] and [11/00/00]

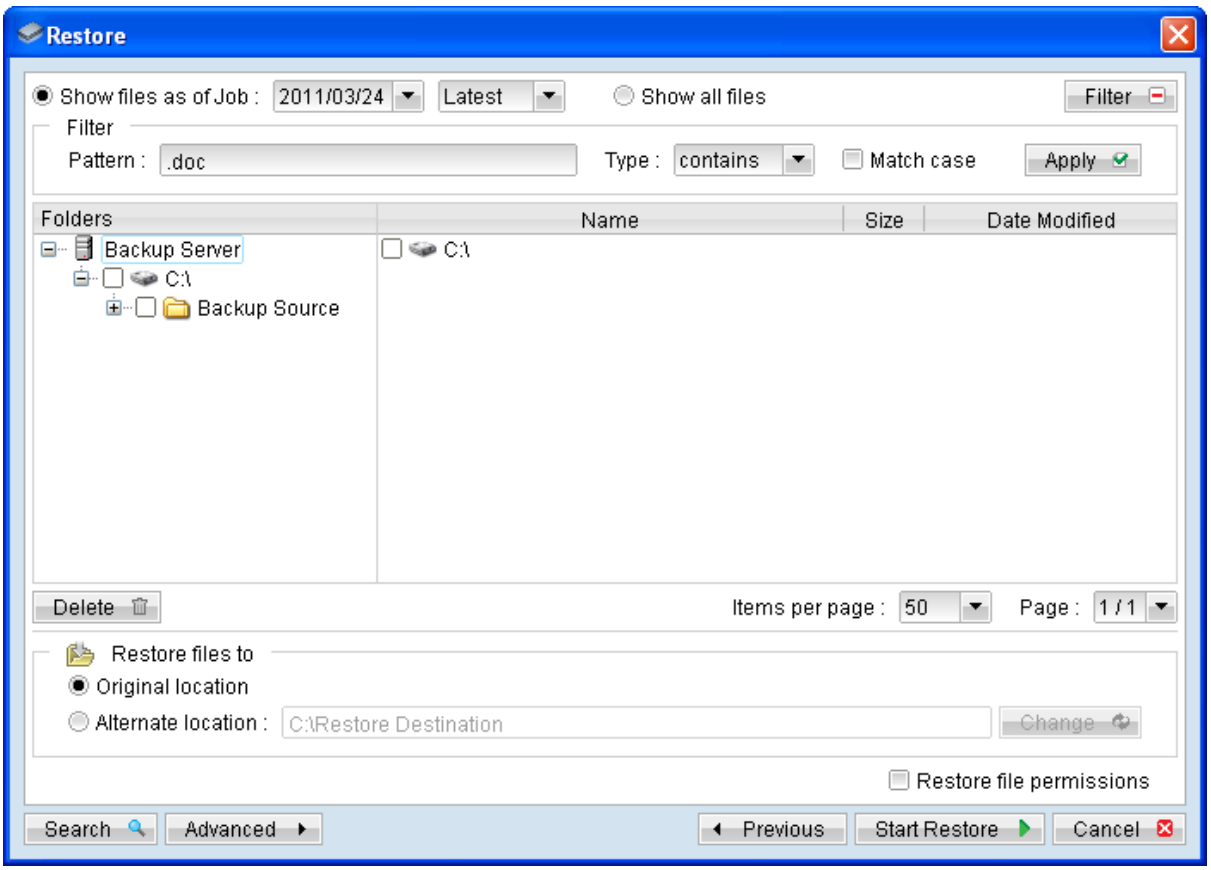
Alternatively, select the [Show all files] to display all files available for restore.

For restore to the original location on the client machine, select the [Original location] radio button.

For restore to an alternate location, select the [Alternate location] radio button, and click [Change] to change the directory path which you would like to restore to.

8.1.1.1 Filter

Click on the [Filter] button to expand the filter option.



Menu Items	Description
Pattern	Input box for entering the pattern of files that you would like to show. Note: Backup filter is case sensitive.
Type	Dropdown menu for selecting the type of pattern, they includes: [contains] [exact] [starts with] [ends with]
Match case	Checkbox to enable or disable case sensitivity.
Apply	Click to apply the filter settings.

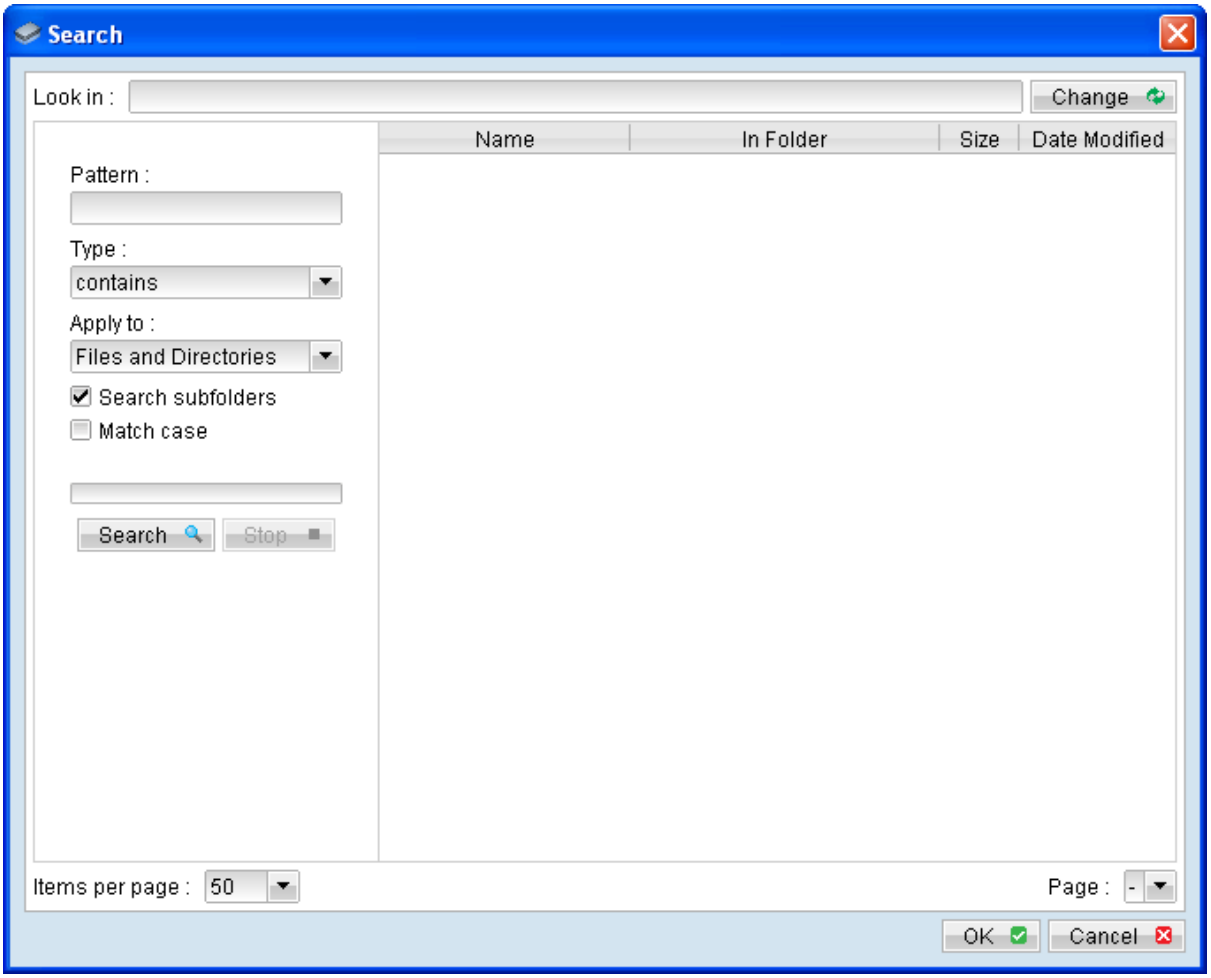
*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

The [Filter] option can be used to restore only files that follow a certain pattern. For example, Words document file with .doc extension.

Enter .doc into the [Pattern] textbox, select [ends with] from the [Type] dropdown menu, and then click [Apply].

8.1.2.1 Search

Click on the [Search] button to open the filter menu.



Menu Items	Description
Look in	Click on the [Change] button to browse to the search destination.
Pattern	Input box for entering the pattern of files that you would like to search for.
Type	Dropdown menu for selecting the type of pattern, they includes: [contains] [exact] [starts with] [ends with]

Apply to	Dropdown menu for selecting if the search is applied to: [Files and Directories] [Files only] [Directories]
Search subfolders	Click to enable or disable search on the subfolders of the selected [Look in] directory.
Match case	Checkbox to enable or disable case sensitivity.
Search	Click to begin the search.
Stop	Click to stop the search process.

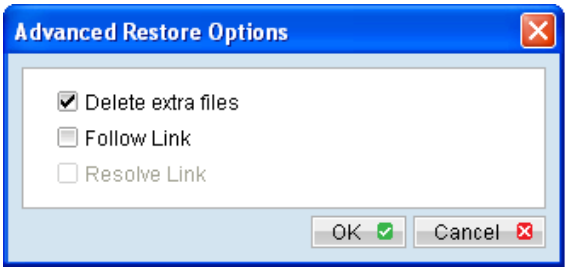
*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

The [Search] option can be used to locate a directory or file within a backup set with large amount of data. When the search is completed, user can select the data for restore in the search menu.

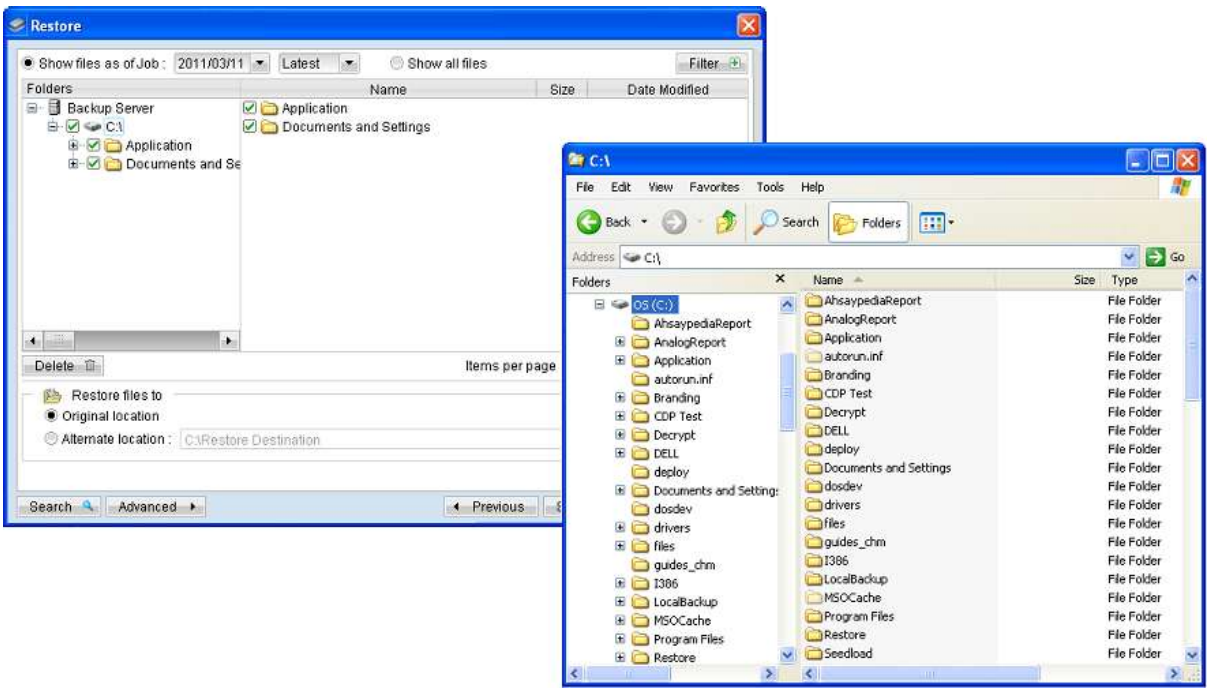
For restore that follow a certain pattern, for example, Microsoft Words document file that ends with .doc only. Enter the pattern .doc into the [Pattern] textbox, select type [ends with] from the [Type] dropdown menu, and click [Apply].

8.1.3.1 Delete extra files

Click on the [Advanced] button, select the [Delete extra files] checkbox to enable the delete extra file option.



When the [Delete extra files] option is enabled, the restore process will attempt to synchronize the selected restore source with the restore destination.

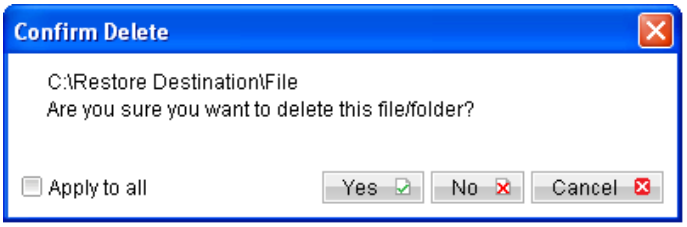


In the image above, where C:\ is selected as the restore source, and [Original location] is selected as the restore destination.

The restore process will attempt to synchronize the restore destination (current C:\ on the client machine) with the restore source (C:\ that is backed up on the backup server).

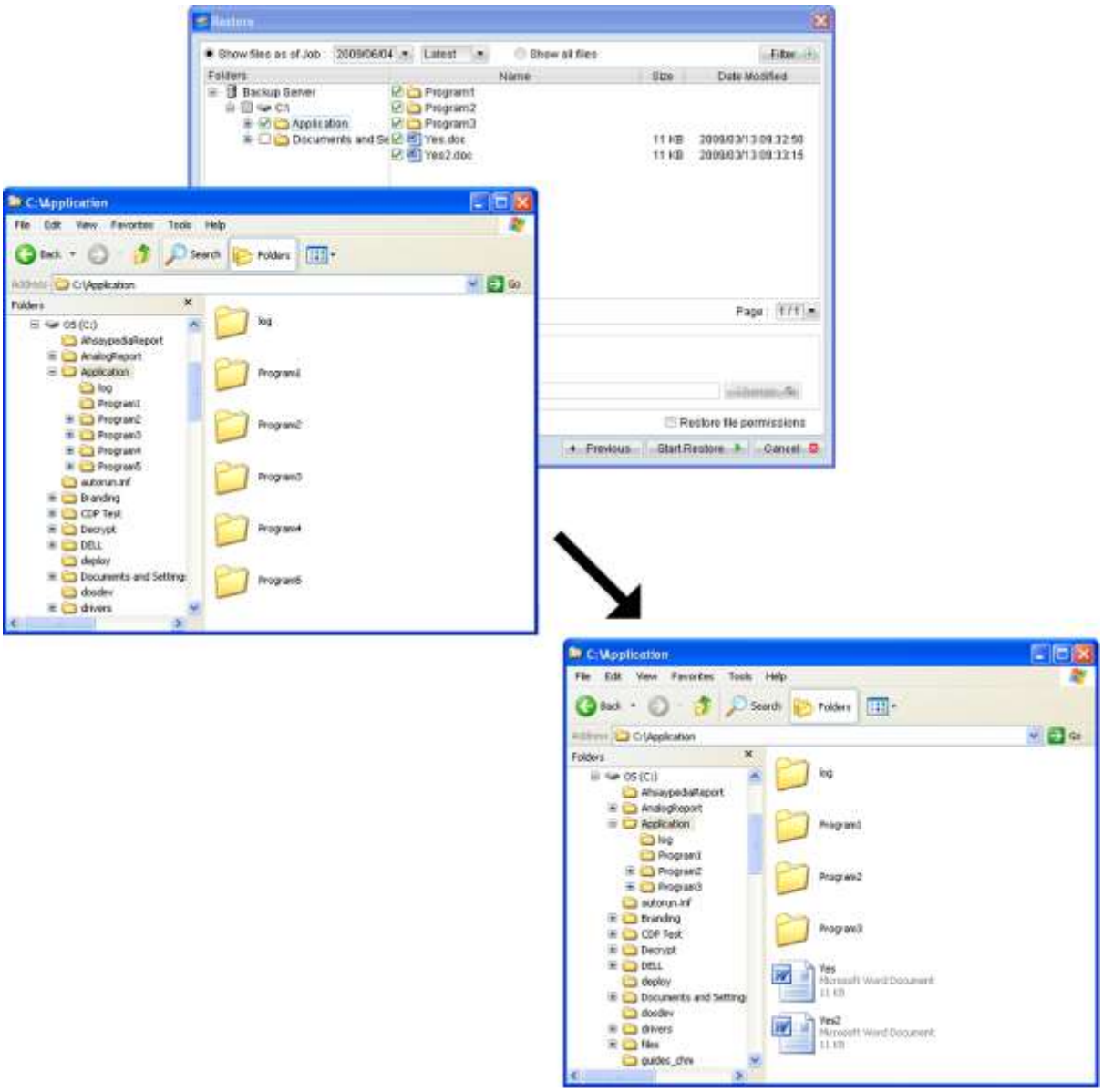
Specifically, the restore process will restore the Application, Documents and Settings folders and the data within, and then delete all other data on C:\ to mirror the restore source and destination.

Prior to the data synchronization, the backup application will prompt for confirmation:



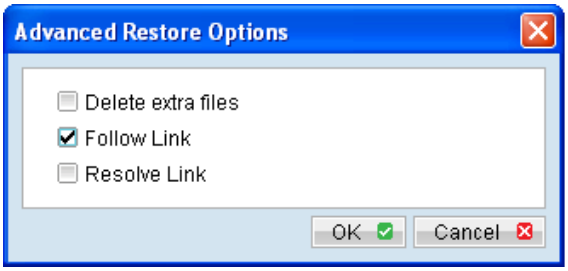
When using the [Delete extra files] option, please select the lowest possible child directories or files, instead of the highest parent directories for synchronization.

To demonstrate, assuming that you want to synchronize the restore destination (e.g. C:\Application) with the backed up C:\Application folder (restore source), select the Application folder, instead of the C:\ for restore.



8.1.4.1 Follow Link

Click on the [Advanced] button, select the [Follow Link] checkbox to enable the follow link option.



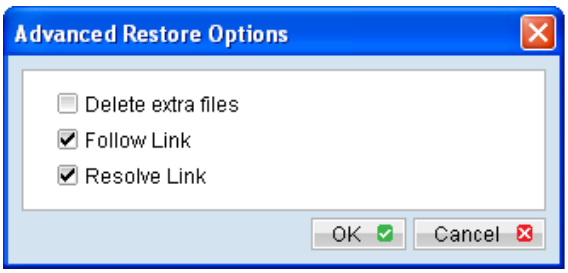
When the follow link option is enabled, not only is the symbolic link or junction point restored, and directories and files that the junction point links to will also be restored.

The following table summarizes the outcome when a restore is performed with different options.

Follow Link	Restore to	Action
Enabled	Original Location	Junction points are restored to the original location. Follow Link option enabled for backup - Target directories and files are restored to the original location. Follow link option disabled for backup - Target directories and files are not restored.
	Alternate Location	Junction points are restored to the location specified. Follow Link option enabled for backup - Target directories and files are restored to the location specified. Follow link option disabled for backup - Target directories and files are not restored.
Disabled	Original Location	Junction points are restored to the original location. No data is restored to the junction point's destination.
	Alternate Location	Junction points are restored to the location specified. No data is restored to the junction point's destination.

8.1.5.1 Resolve Link

Click on the [Advanced] button, select the [Resolve Link] checkbox to enable the resolve link option.



Note that the resolve link option is only available when the restore destination is configured to [Alternate location], and [Resolve Link] must be used in conjunction with the [Follow Link] option.

When the resolve link option is enabled, the junction point would be restored, and directories and files that the junction point links to will also be restored.

The following table summarizes the outcome when a restore is performed with different options.

Resolve Link	Action
Enabled	Junction points are restored to the alternate location specified, with its target directories and files also restored to the location specified in their relative path. Target of the junction is updated to the new relative path. In other words, junction now points to the new alternate location).
Disabled	Junction points are restored to the alternate location specified, with its target directories and files also restored to the location specified in their relative path. Target of the junction is not updated to the new relative path. In other words, junction now points to the original location.

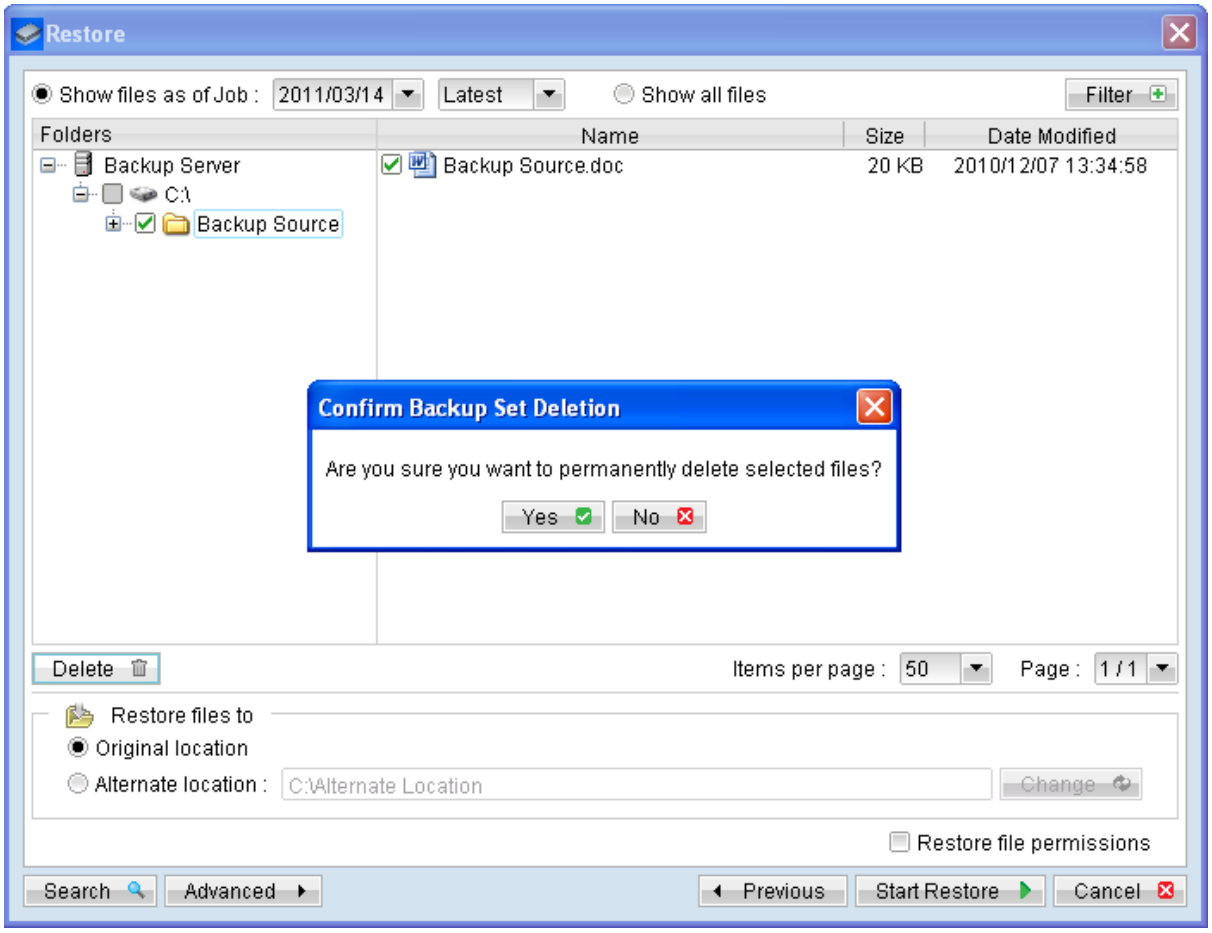
8.1.6.1 Delete backed up directories and files on backup server

Click on the [Delete] button to delete backed up data that reside on the backup server.

This option is useful for removing backed up directories or files on server that is no longer required.

Select the checkboxes beside the corresponding directories or files that you would like to delete, and click [Delete].

Prior to the data removal, the backup application will prompt for confirmation:



Important:
Files will not be available for restore after they are deleted from the backup server.

8.2 How to start a restore

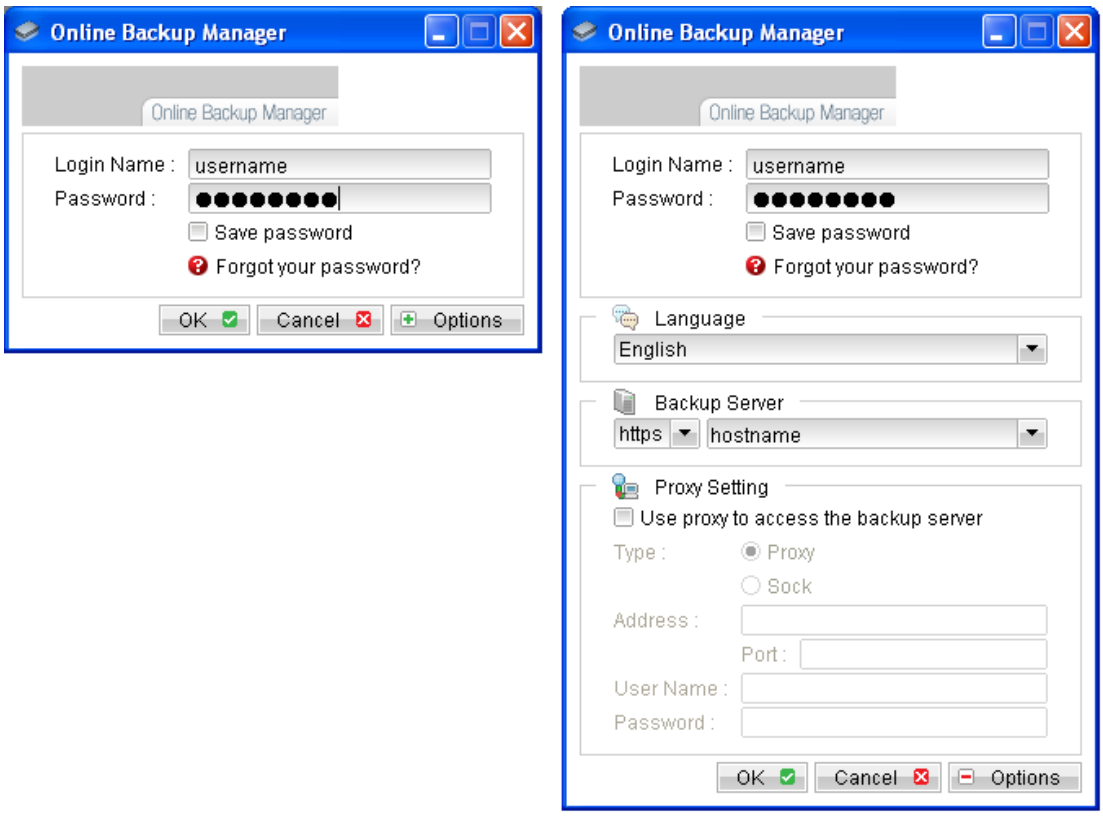
There are three methods for restoring data:

- OBM user interface
- Web console interface
- Decrypt File Wizard for physical data copied from OBS

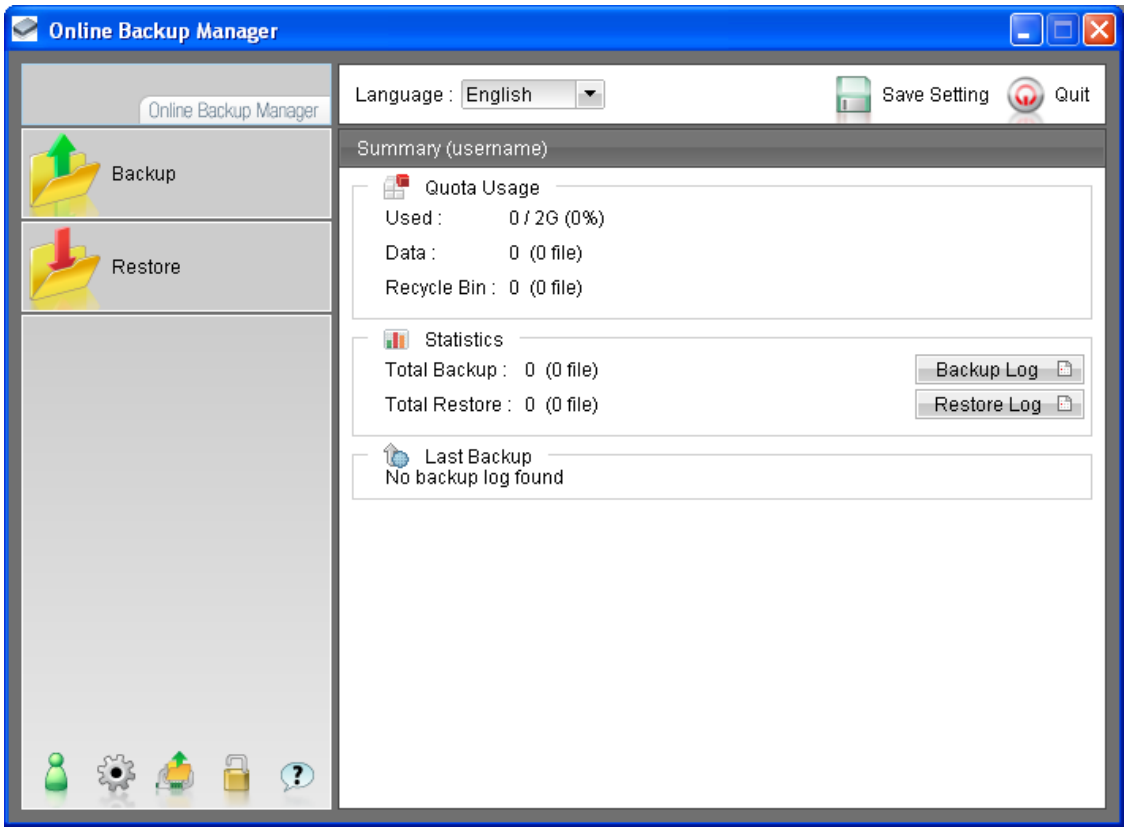
8.2.1 Restore using the OBM user interface

Refer to the following steps for restore using the backup application's user interface:

1. Login to the backup application's user interface.



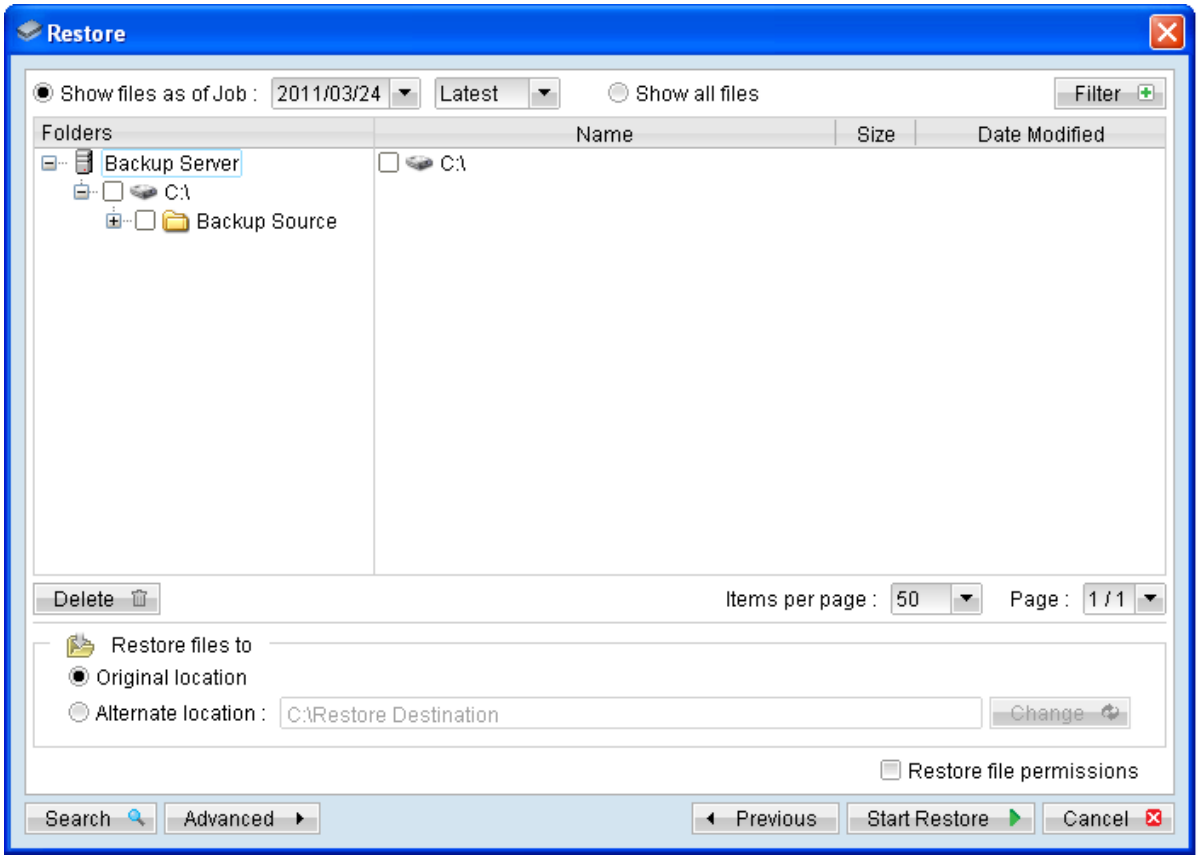
2. Click on the [Restore] button on the backup application's main window to open the Restore Menu.



3. Select the [Show files as of Job] to display files available as of a particular backup job.

   To display the files available for restore since the backup job performed on 11:00 AM, Mar 11th, 2011, select [Show files as of Job], [2011/03/11] and [11:00:00]

   Select the [Show all files] to display all files available for restore.



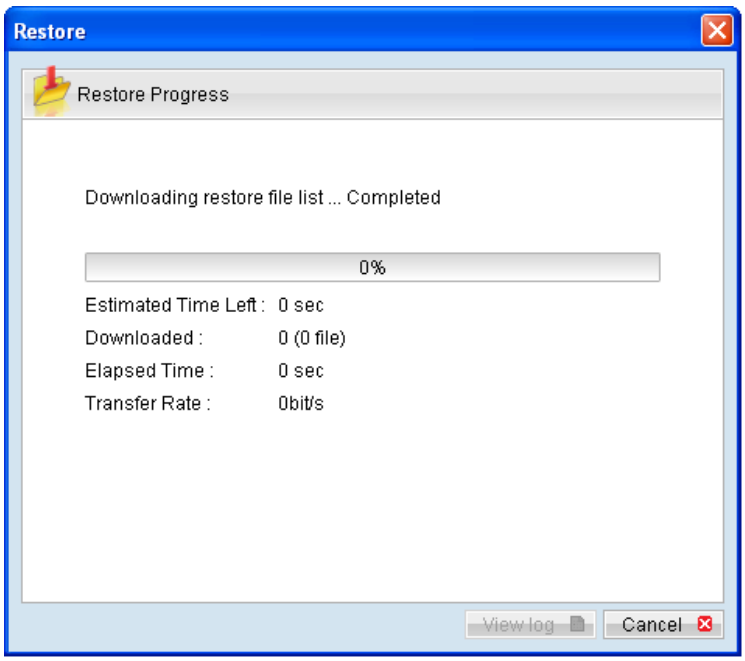
4. Expand the directories by selecting the ⊞ button beside a folder.

5. Make use of the other options such as [Filter], [Search] and [Advanced] option available, more details can be found in the sections above.

6. For restore to the original location on the client machine, select the [Original location] radio button.

   For restore to an alternate location, select the [Alternate location] radio button, and click [Change] to change the directory path which you would like to restore to.

7. Click [Start Restore] to begin the restore process.

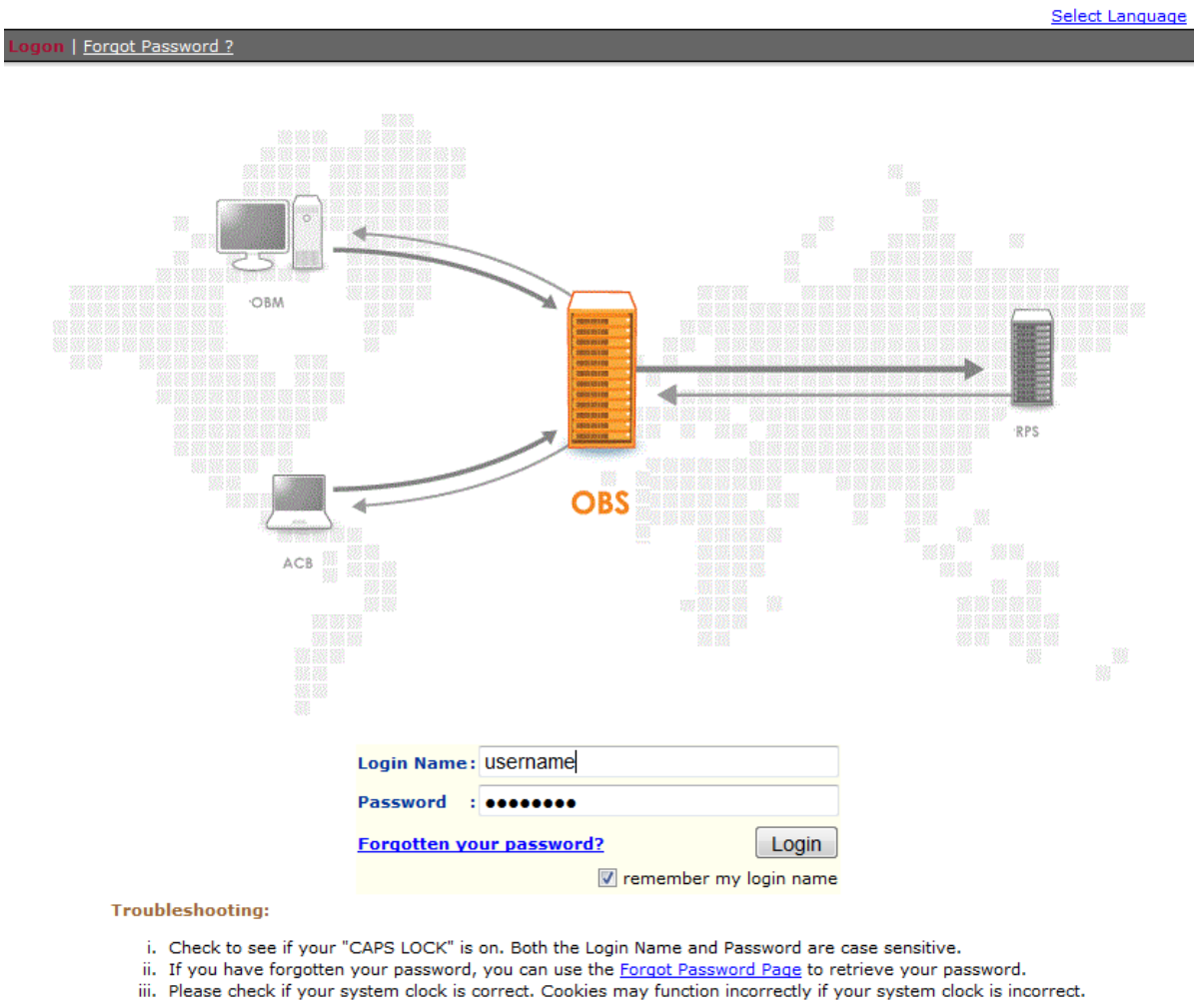

Restore
Restore Progress
Downloading restore file list ... Completed
0%
Estimated Time Left : 0 sec
Downloaded : 0 (0 file)
Elapsed Time : 0 sec
Transfer Rate : 0bit/s
View log
Cancel

8.2.2 Restore using the web interface

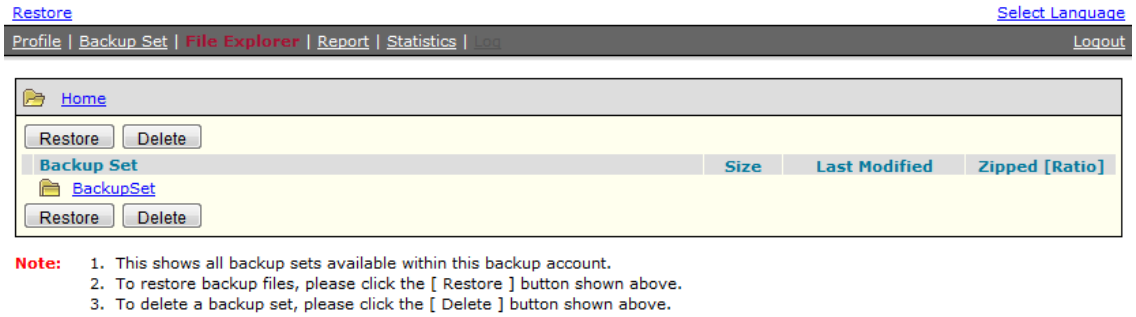
Refer to the following steps for restore using the web interface:

Note:
For restore of a large amount of data, it is recommended to restore using the OBM user interface instead of the web restorer applet.

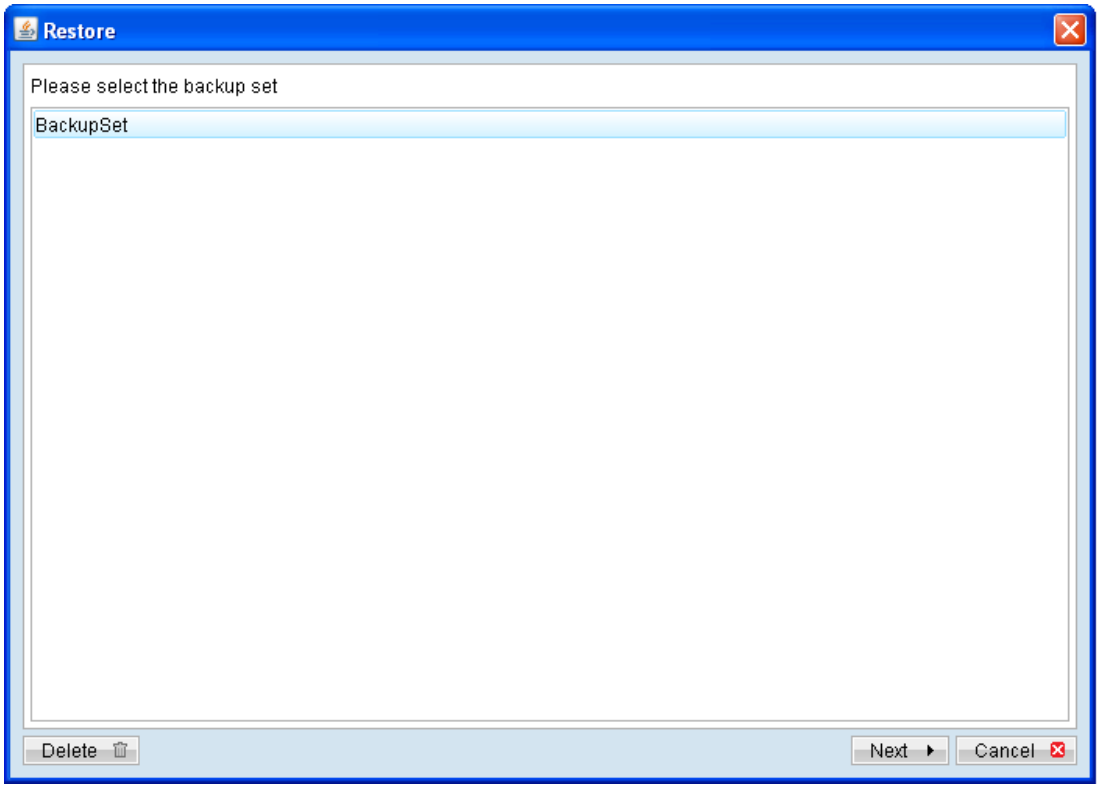
1. Login to the web interface.


Select Language
Logon | Forgot Password ?
OBM
OBS
RPS
ACB
Login Name: username
Password : ••••••••
Forgotten your password?
Login
remember my login name
Troubleshooting:
i. Check to see if your "CAPS LOCK" is on. Both the Login Name and Password are case sensitive.
ii. If you have forgotten your password, you can use the Forgot Password Page to retrieve your password.
iii. Please check if your system clock is correct. Cookies may function incorrectly if your system clock is incorrect.

2. Click on the [File Explorer] tab at the top menu of the web interface.



3. Click on the [Restore] button to open the web restorer applet:

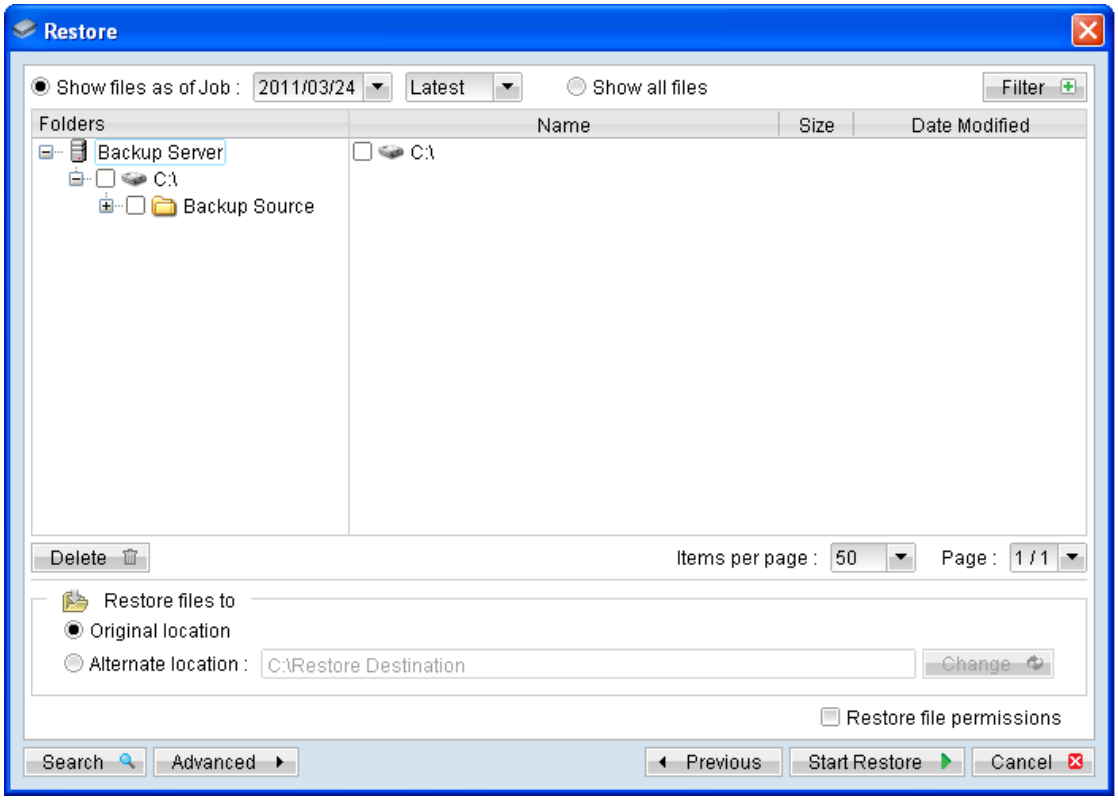


4. Select the corresponding backup set and press [Next]

5. Select the [Show files as of Job] to display files available as of a particular backup job.

For example, select [Show files as of Job], [2011/03/11] and [11:00:00] to display the files available for restore since the backup job performed on 11:00am of Mar 11th, 2011.

Select the [Show all files] to display all files available for restore.



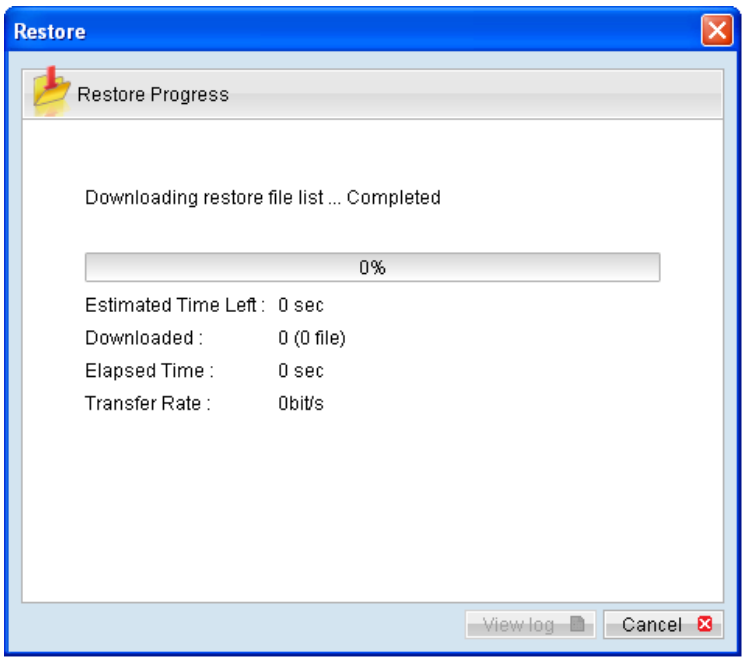
6. Expand the directories by selecting the ⊞ button beside a folder.

7. Make use of the other options such as [Filter], [Search] and [Advanced] option available, more details can be found in the earlier sections of this guide.

8. For restore to the original location on the client machine, select the [Original location] radio button.

   For restore to an alternate location, select the [Alternate location] radio button, and click [Change] to change the directory path which you would like to restore to.

9. Click [Start Restore] to begin the restore process.



8.2.3 Restore using Decrypt File Wizard

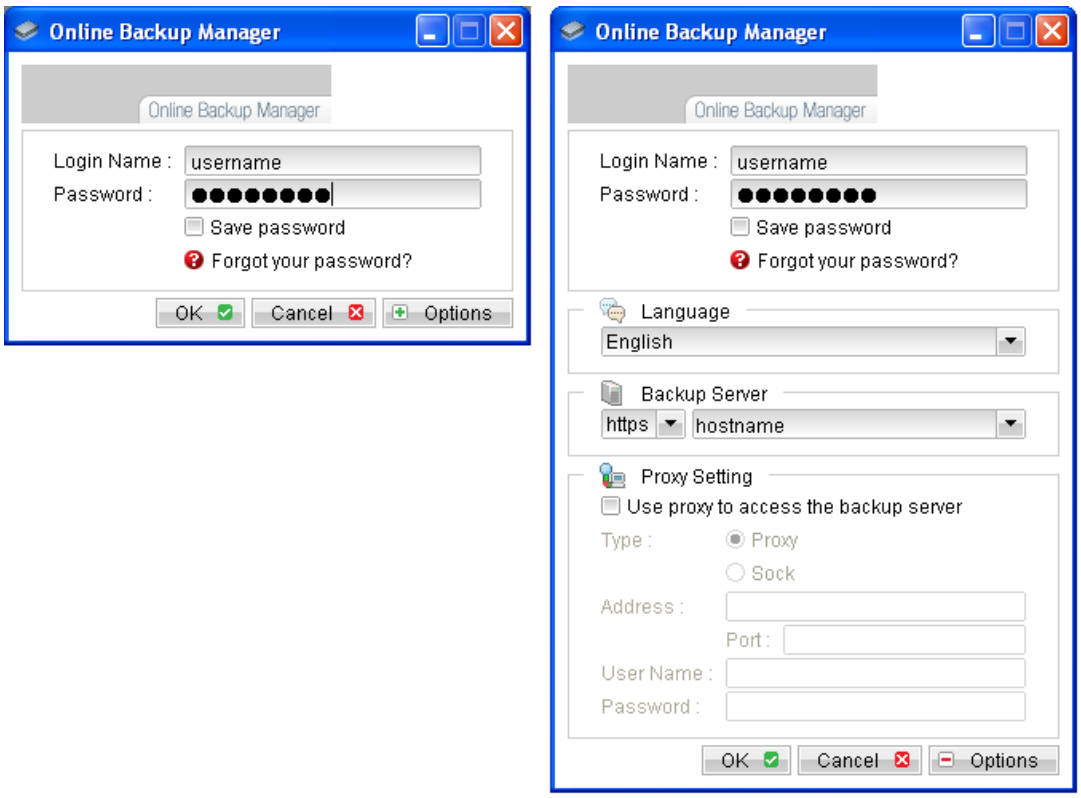
Data stored on the backup server can be copied onto a removable hard disk (or other storage medium) for direct restore on the client computer, bypassing the network bottleneck. This is especially useful for restore of large backup set.

However, as data stored on the backup server are compressed and encrypted for security purposes, a utility called Decrypt File Wizard must be used to decrypt the data.

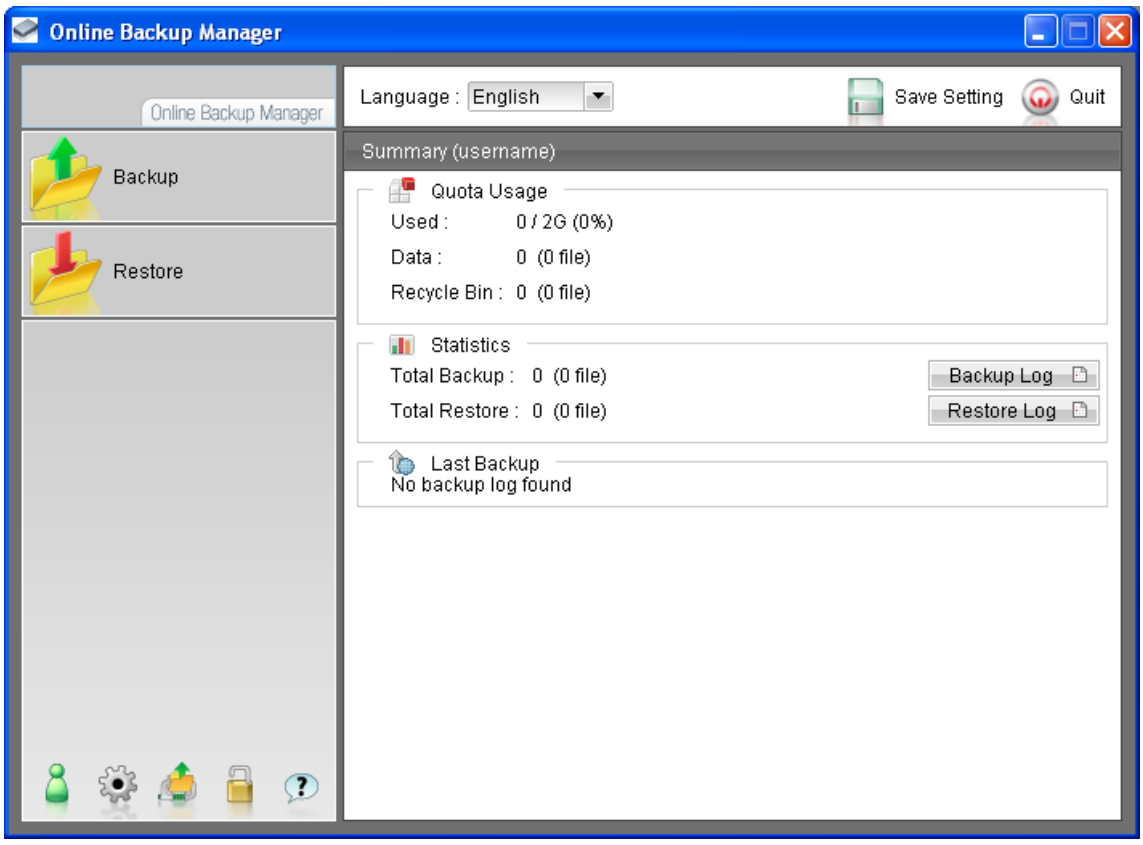
Refer to the following steps for restore using Decrypt File Wizard:

1. Connect the removable hard disk with the data to your computer.

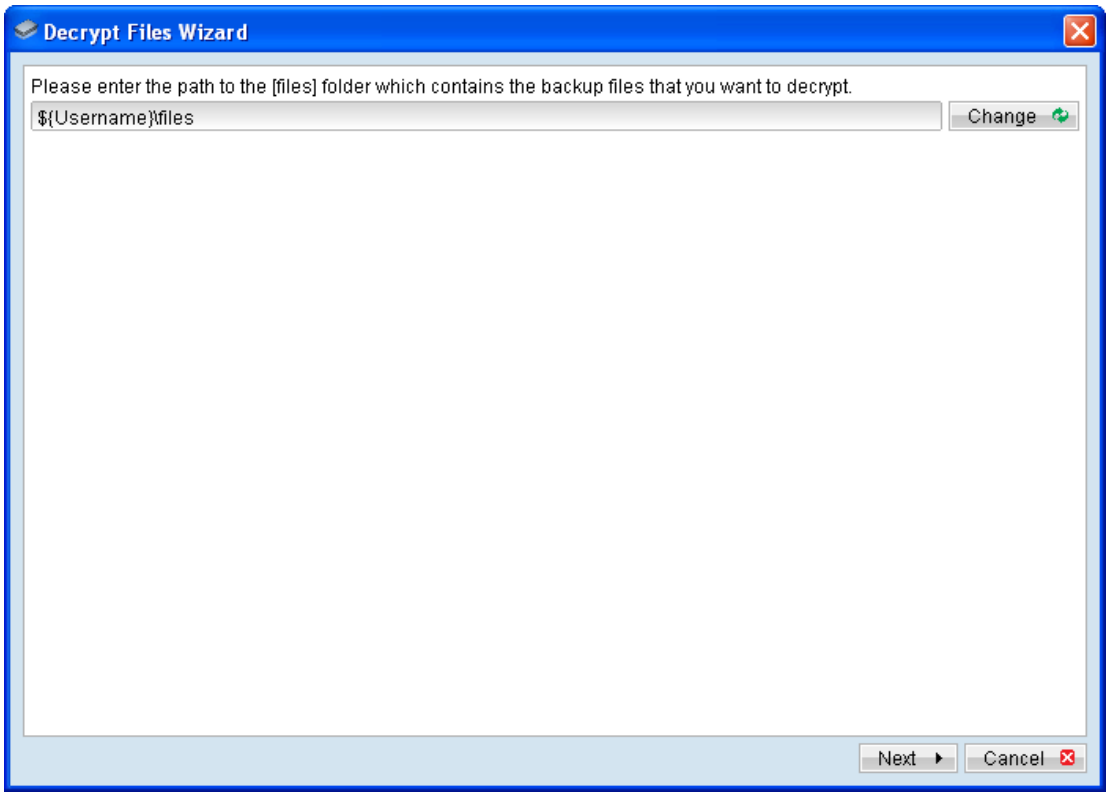
2. Login to the backup application's user interface.



3. Click on the [Decrypt File Wizard] button on the backup application's main window to open the Decrypt File Wizard.



4. Select the [Change] button and browse to the [files] directory of the copied data, and click [Next].

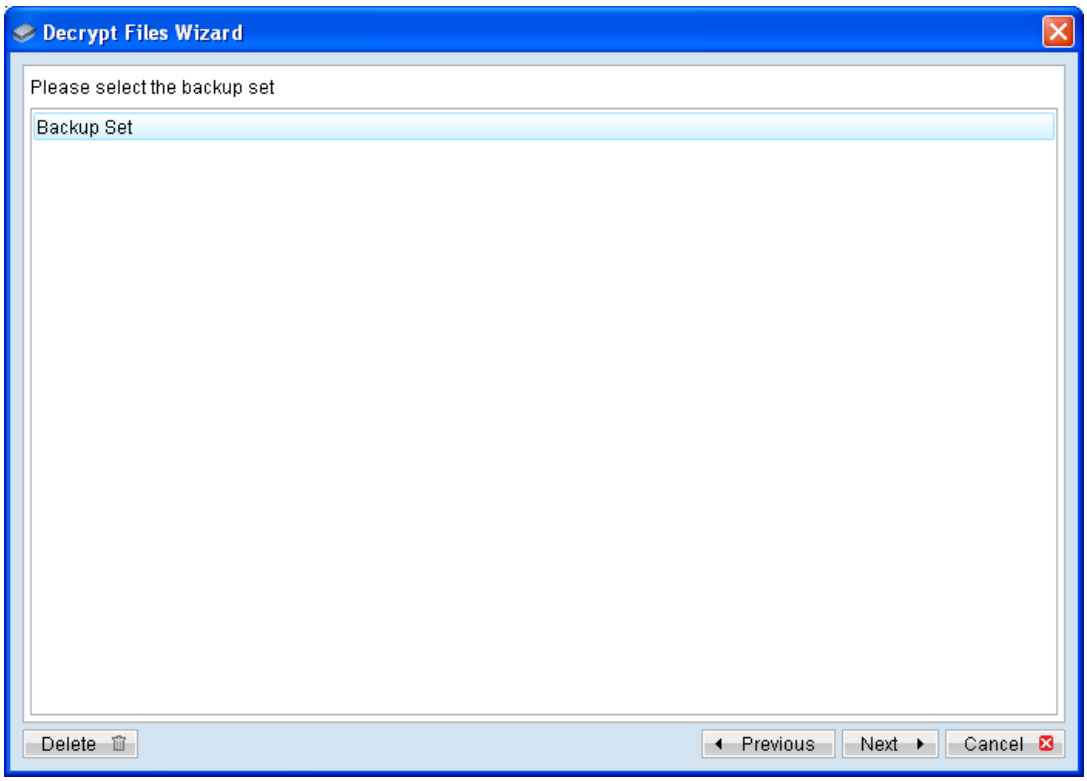

Decrypt Files Wizard
Please enter the path to the [files] folder which contains the backup files that you want to decrypt.
${Username}\files
Change
Next
Cancel

Note:
Data copied onto the removable hard disk must be in the same directory structure as they are on the backup server, which is:

${Username}\files

Please contact your service provider if you cannot locate the [files] directory.

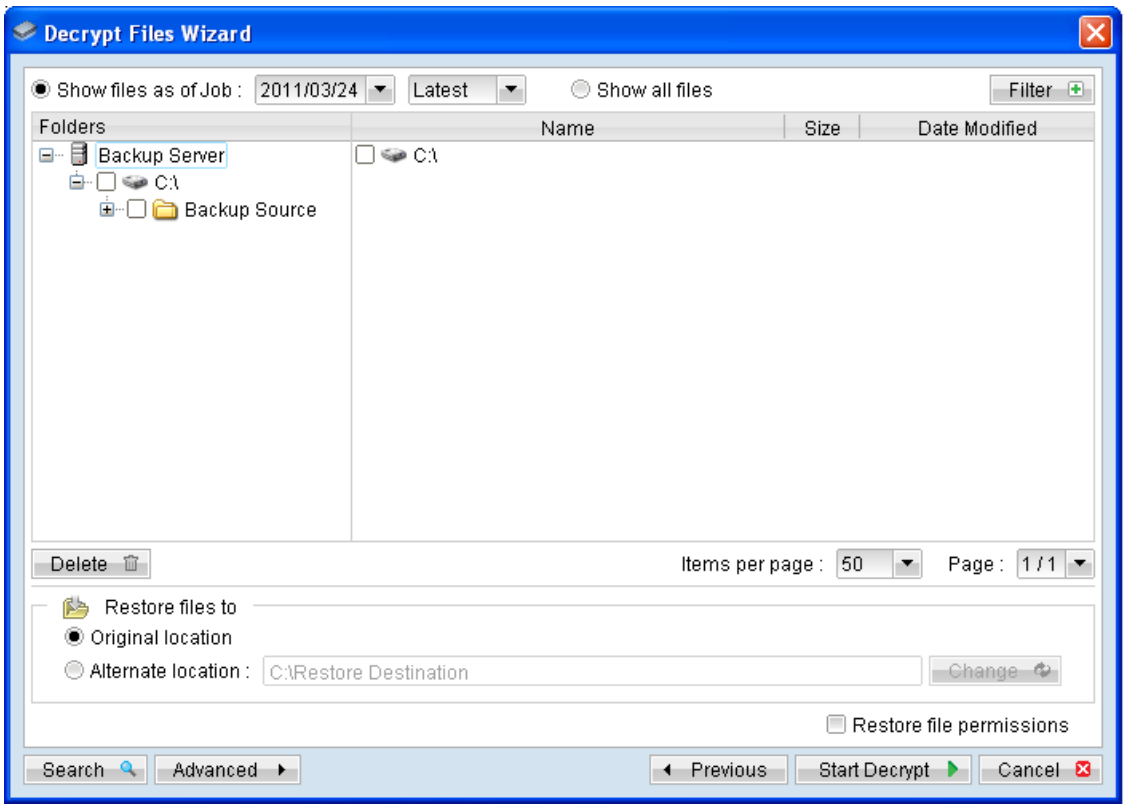
5. Select the corresponding backup set and press [Next]



6. Select the [Show files as of Job] to display files available as of a particular backup job.

   For example, to display the files available for restore since the backup job performed on 11:00 AM, Mar 11th, 2011. Select [Show files as of Job], [2011/03/11] and [11:00:00]

   Select the [Show all files] to display all files available for restore.



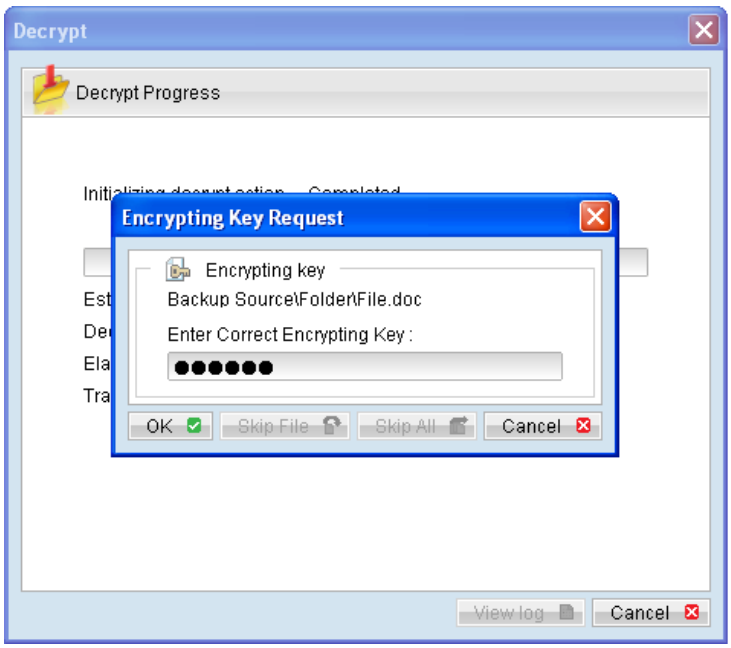
7. Expand the directories by selecting the ⊞ button beside a folder.

8. Make use of the other options such as [Filter], [Search] and [Advanced] option available, more details can be found in the sections above.

9. For decrypt to the original location on the client machine, select the [Original location] radio button.

   For decrypt to an alternate location, select the [Alternate location] radio button, and click [Change] to change the directory path which you would like to restore to.

10. Click [Start Decrypt] to begin the decrypt process.



8.3 IP restriction for restore using the web interface

IP address restriction can be imposed on the backup server to restrict computer with un-authorized IP address from restoring data using the web interface.

Please consult your service provider for more information on this option.

9 In-file delta technology

This chapter describes what In-file delta technology is and how it can be used to reduce size of backup.

9.1 Overview

In-file delta technology is an advanced data block matching algorithm with the intelligence to pick up changes (delta) of file content between two files.

Using this algorithm, daily backup of large files over low-speed internet connection is made possible because it requires only the changes of information since the last backup to be sent over (assuming that the full backup of the file has been saved on the backup server already).

This is what will happen in the backup of a 10 GB Outlook.pst file when it is backed up by OBM with In-file delta technology:

1. The whole file (10 GB) with its checksum file, are backed up to the backup server. This can be done directly through the internet or indirectly using the seed loading utility

2. When the backup runs again later (sub-sequence backup), OBM will download a checksum listing of all data blocks of the full backup file (or last incremental backup file) from the backup server and use it to pick up all changes that have been made to the current Outlook.pst file.

3. Changes detected are then saved in a delta file which is uploaded to the backup server. A new checksum file is generated and is also uploaded. (This delta file is assumed to be small because the content of PST files doesn't change a lot during daily usage).

4. Sub-sequent backups of this 10 GB Outlook.pst file will go through step 2 and step 3 again. As explained, only a small delta file and checksum file will be uploaded to the backup server.

5. With In-file delta technology, daily backing up of large file over low-speed internet connection is now possible.

Incremental In-file delta
Incremental Delta will facilitate ease of backup.

The delta is generated by comparing with the last uploaded full or delta file. Delta generated with this method is smaller and uses the least bandwidth.

However, for restoration, the full file and all deltas up to the required point-in-time are required to be restored and merged.

For example:
This is what will happen in the backup of a 10 GB Outlook.pst file with 100 MB increment each day.

After the initial full backup, the backup application would continue to generate and upload delta instead of the full file until one of the following two rules are true:

- Number of delta files generated (since the last full backup) exceeded the [No. of Delta] setting.

- The delta ratio (ratio of delta file size against the full file size) exceeded the [Delta Ratio] setting.

With incremental delta, delta generated by comparing the current file with the last uploaded file (full or delta) is around 100 MB.

Since the delta file size is about 100 MB daily, delta ratio of 1% would not trigger a full file upload.

Instead, OBM will continue to generate and upload delta files until day 102 (full file uploaded on day 1) when the number of deltas generated exceeds the [No. of Delta] setting.

All delta files are generated with respect to changes made since the last incremental or full backup. This means that the last full backup file and ALL incremental delta backup files are required to restore the latest snapshot of a backup file.

Differential In-file delta
Differential Delta will facilitate ease of restore.

The delta is generated by comparing with the last uploaded full file only. Delta generated with this method will grow daily and uses more bandwidth.

However, for restoration, the full file and a single delta is required to be restored and merged.

For example:
This is what will happen in the backup of a 10 GB Outlook.pst file with 100 MB increment each day.

After the initial full backup, the backup application would continue to generate and upload delta instead of the full file until one of the following two rules are true:

- Number of delta files generated (since the last full backup) exceeded the [No. of Delta] setting.
- The delta ratio (ratio of delta file size against the full file size) exceeded the [Delta Ratio] setting.

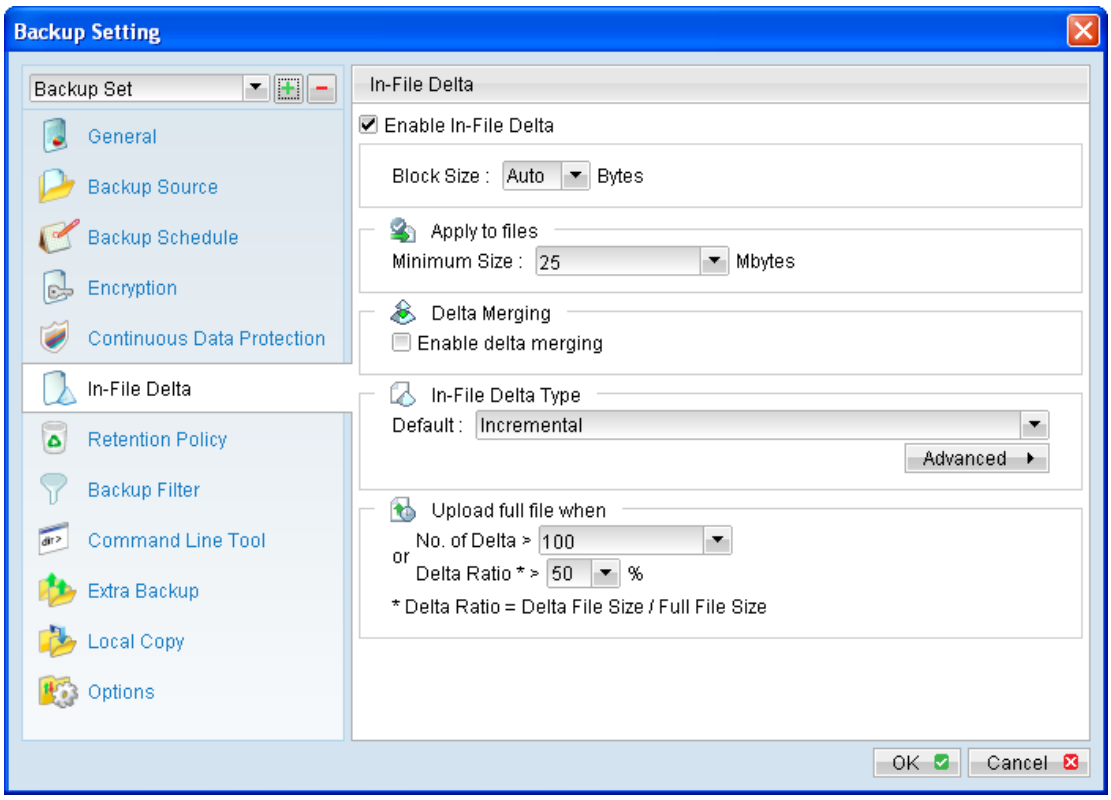
With differential delta, delta generated by comparing the current file with the last full file is about 100 MB for the 1st delta, 200 MB for the 2nd delta, and 300 MB for the 3rd delta (increment of 100 MB per day).

Since the delta file size increase by 100 MB per day, OBM will continue to generate and upload delta files until day 52 (full file uploaded on day 1) when the delta ratio exceeds the [Delta Ratio] setting:

Delta file size of approximately 51 × 100 MB = 5.1 GB.

All delta files are generated with respect to changes made since the last full backup. This means that only the last full backup file and the last delta file are required to restore the latest snapshot of a backup file.

*In the event of corrupted delta file, only one particular snapshot of the file is non-restorable. All other snapshots with its delta would remain intact.



9.1.1 Block Size

[Block Size] defines the size of block used when detecting changes between last full or delta file and the file to be backed up.

In general:

In-file delta backup with small block size:
- Produce a smaller delta file due to a more precise comparison
- Require more processing power on the client machine
- Comparison may take longer to complete

In-file delta backup with large block size:
- Produce a larger delta file due to a less precise comparison
- Require less processing power on the client machine
- Comparison will complete faster

For most cases, the default setting [Auto] will select the optimal block size for each file (depending on the size of the file).

9.1.2 Apply to files (Minimum Size)

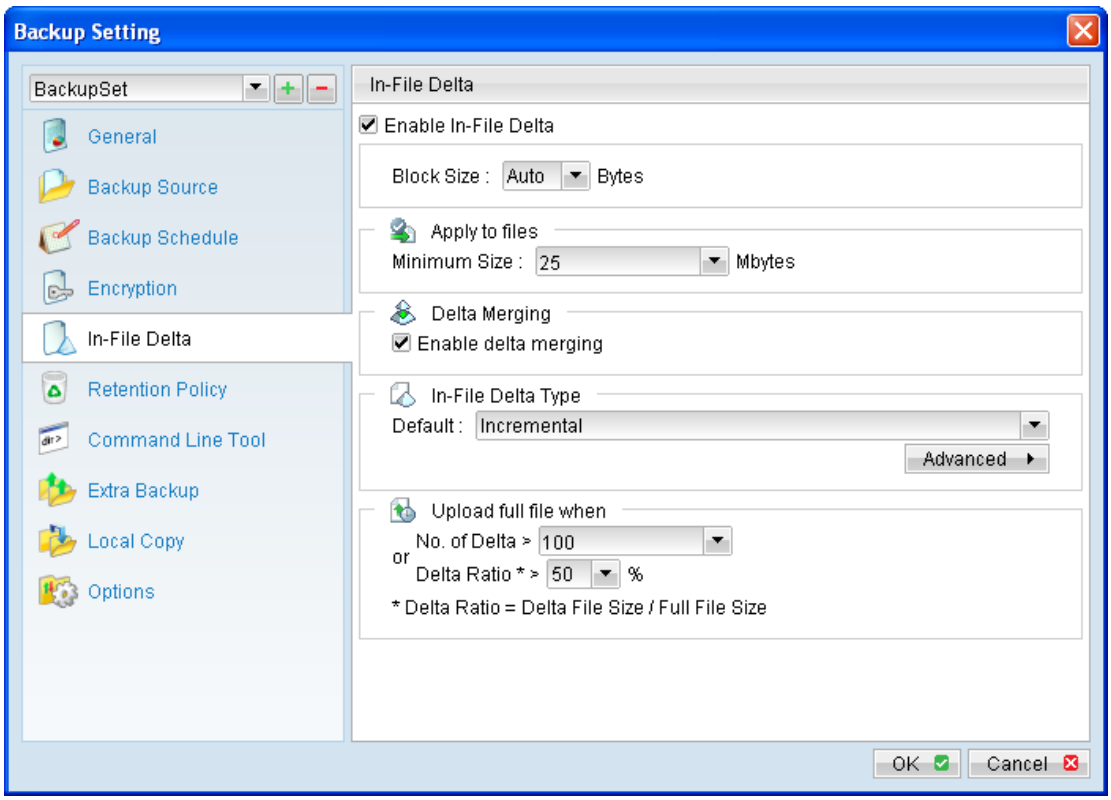
[Apply to files (Minimum Size)] defines the smallest file size a file must have before the use and application of In-file delta technology.

If the size of a file that is being backed up is smaller than the [Minimum File Size] setting, In-file delta technology will not be applied to this file and the whole file will be uploaded to the backup server.

It is not necessary to perform In-file delta backup on small files because backing up the whole file does not take long. Backing up the whole file instead reduces the time required to restore the file..

9.1.3 Delta Merging (Enable delta merging)

[Delta Merging (Enable delta merging)] defines whether to enable the delta merge feature for the corresponding backup set.



To enable the delta merging feature, select the [In-File Delta] tab in the [Backup Setting] menu, and select the checkbox beside [Enable delta merging].

9.1.1.3 Overview

The delta merge feature combines the full and delta files (differential or incremental) on OBS into a single full file.

The advantage of using delta merge is it will speed up the restore of files. As a single 'merged' file can be restored faster than a file consisting of full plus related incremental files, which may require a lengthy merging process after restoring to a client machine.

Delta merge can be applied to full and differential or incremental delta files which reside in the data area. The criteria for file merging are governed by the retention policy setting for the backup set.

9.1.2.3 Limitation

The following are limitations of the delta merge feature:

- Delta merge cannot be performed for abnormal backup set with multiple encryption key

- Advanced retention policy cannot be used in conjunction with the delta merge feature.
- The delta merge of differential delta files with the full file, will only apply if there are incremental delta files present in the delta chain.

  Therefore, no delta merge will take place for backup sets with delta merge enabled and in-file delta set to Differential.
- The delta merge feature does not support Local Copy backup.

9.1.3.3 Delta merge policy

The delta merge process relies on the retention policy setting to decide when to merge delta files with the full file. But delta merge does not apply to files in the retention area. Any backup sets configured with advanced or customized retention policy settings cannot use the delta merge feature.

Any reference to retention policy in the context of delta merge implies delta merge policy. As backup sets enabled with delta merge share a single setting, any changes in retention policy will impact on the availability of snapshots that can be restored from both data and retention area. Before enabling the delta merge feature please review your data restore requirements carefully

9.1.4.3 Delta merging process

A delta merge will take place after a backup job is completed, OBM will only initiate a delta merge request at the end of a backup job.

As part of the request, OBM will upload a copy of the backup set encryption key to OBS which is hashed for security purposes. Once a merge request is received by OBS it will be placed in the delta merge queue, the information in the delta merge queue only exists in memory for security purposes.

As backup sets enabled with delta merge share a single setting, any changes in retention policy will impact on the availability of snapshots that can be restored from both data and retention area.

Important:
Before enabling the delta merge feature please review your data restore requirements carefully.

9.1.5.3 Delta merging example

The following is some simple examples to demonstrate the functionality of the delta merge feature:

Example 1:

The example below shows how delta files are merged into full file using a retention policy (delta merge policy) setting defined as 4 jobs for this backup set.

A full backup file is stored into data area (F) uploaded by Job 1, followed by incremental delta files I_1, I_2, I_3, and I_4. On the completion Job 5 (I_4), the backup application will trigger a delta merge background job to execute the file merging. When the OBS delta merge job runs F + I_1 will be merged to become a merged full file. The data area now contains 4 snapshots including merged full file after file merging.

Retention Policy = 4 Jobs (Delta Merge Policy)

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = I_4 (delta merge initiated)

After job 5 the backup application will initiate a delta merge for Job 1 & Job 2 files.

F (F + I_1) merged full file
I_2
I_3
I_4

Example 2:
The example below shows how delta files are merged into full file using a retention policy (delta merge policy) setting defined as 7 days for this backup set.

A full backup file is stored into data area (F) uploaded on Day 1, followed by incremental delta files I_1, I_2, I_3, I_4, I_5, I_6, I_7, and I_8,. On the completion of the backup job on Day 9 (I_8), the backup application will trigger a delta merge background job to execute the file merging. When the OBS delta merge job runs F + I_1 will be merged to become a merged full file. The data area now contains 8 snapshots including merged full file after file merging.

Retention Policy = 7 Days (Delta Merge Policy):

Day 1 = F
Day 2 = I_1
Day 3 = I_2
Day 4 = I_3
Day 5 = I_4
Day 6 = I_5
Day 7 = I_6
Day 8 = I_7
Day 9 = I_8 (delta merge initiated)

After job on day 9 the backup application will initiate a delta merge for Day 1 & Day 2 files. As the incremental file I_1 has exceeded the 7 day retention policy setting.

F (F + I_1) merged full file
I_2
I_3
I_4
I_5
I_6
I_7
I_8

Example 3:
This example below shows what happens when there are multiple backup jobs occurring which generates incremental delta files within a 24 hour period.

A full backup file is stored into data area (F) uploaded by Job 1, followed by incremental delta files I_1, I_2, I_3, and I_4. On the completion Job 5 (I_4), the backup application will trigger a delta merge background job to execute the file merging. When the OBS delta merge job runs F + I_1 will be merged to become a merged full file.

Retention Policy = 4 Jobs (Delta Merge Policy)

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = I_4 (delta merge initiated)
Job 6 = I_5
Job 7 = I_6

After job 5 the backup application will initiate a delta merge for Job 1 & Job 2 files. If after the delta merge there are further incremental uploads, e.g. Job 6 and Job 7. These increment files will not be merged by OBS as a delta merge jobs has already taken place within the last 24 hours. The data area now contains 6 jobs, which exceeds the delta merge policy of 4 jobs

F (F + I_1) merged full file
I_2
I_3
I_4
I_5
I_6

OBS will merge the extra incremental files, when the next backup job completes 24 hours after the last delta merge. OBS will merge all the delta files which have exceeded the backup set delta merge policy.

Example 4:
The example below shows how differential and incremental delta files are merged into full file using a retention policy (delta merge policy) setting defined as 4 jobs for this backup set.

A full backup file is stored into data area (F) uploaded by Job 1, followed by incremental and differential delta files I_1, I_2 I_3 and D_1.

Retention Policy = 4 Jobs (Delta Merge Policy)

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = D_1 (delta merge initiated)

After Job 5 the backup application will initiate a delta merge for Job 1 & Job 2. Unfortunately, differential delta D_1 is found in delta chain, this creates delta merge stoppage, the files in Job 1 and Job 2 will not be merged.

The backup job continues with subsequent incremental backups (I_4, I_5 and I_6).

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = D_1 (delta merge is initiated and stopped)
Job 6 = I_4 (delta merge is initiated and stopped)
Job 7 = I_5 (delta merge is initiated and stopped)
Job 8 = I_6 (delta merge is initiated)

After Job 8 the backup application will initiate a delta merge, OBS will merge the full file (F) uploaded in Job 1 with the differential delta D_1 uploaded in Job 5 to form the new full file (As the D_1 differential includes changes in I_1 + I_2 + I_3). The incremental files I_1 + I_2 + I_3 will be moved to the retention area, as they have already exceeded the retention policy of 4 jobs. These files will be purged on the next retention policy job.

After the delta merge has completed the follow files will be available for restore.

F (F + D_1)
I_4
I_5
I_6

Example 5:

The example below shows how delta merge handles multiple differential delta files using a retention policy (delta merge policy) setting defined as 4 jobs for this backup set.

A full backup file is stored into data area (F) uploaded by Job 1, followed by incremental and differential delta files I_1, I_2 I_3 and D_1.
Retention Policy = 4 Jobs (Delta Merge Policy)

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = D_1 (delta merge initiated)

After Job 5 the backup application will initiate a delta merge for Job 1 & Job 2. Unfortunately, differential delta D_1 is found in delta chain, this creates delta merge stoppage, the files in Job 1 and Job 2 will not be merged.

The backup job continues with subsequent differential delta backups (D_2 and D_3) and incremental delta backups (I_4, I_5, and I_6).

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = D_1 (delta merge is initiated and stopped)
Job 6 = D_2 (delta merge is initiated and stopped)
Job 7 = D_3 (delta merge is initiated and stopped)
Job 8 = I_4 (delta merge is initiated and stopped)
Job 9 = I_5 (delta merge is initiated and stopped)
Job 10 = I_6 (delta merge is initiated)

After Job 10 the backup application will initiate a delta merge, OBS will merge the full file (F) uploaded in Job 1 with the latest differential delta D_3 uploaded in Job 7 to form the new full file (As the D_3 differential includes changes in I_1 + I_2 + I_3 + D_1 + D_2). The files I_1 + I_2 + I_3 + D_1 + D_2 will be moved to the retention area, as they have already exceeded the retention policy of 4 jobs. These files will be purged on the next retention policy job.

After the delta merge has completed the follow files will be available for restore.

F (F + D_3)
I_4
I_5
I_6

9.1.4 In-File Delta Type

The [In-file Delta Type] setting defines the way In-File Delta files are handled. There are two different versions as follows:

Incremental In-File Delta
All delta files are generated with respect to changes made since the last incremental backup. This means that the last full backup file and all related incremental delta backup files are required to restore the latest snapshot of a backup file.

The full backup file, its checksum file and all incremental delta files are always stored in the data area. This means that these files are not affected by the setting of the retention policy and will always be kept on the backup server. However, for backup sets with delta merge enabled, the retention policy setting is also used by the delta merge feature to determine when OBS will merge the full and incremental delta files into a new full file.

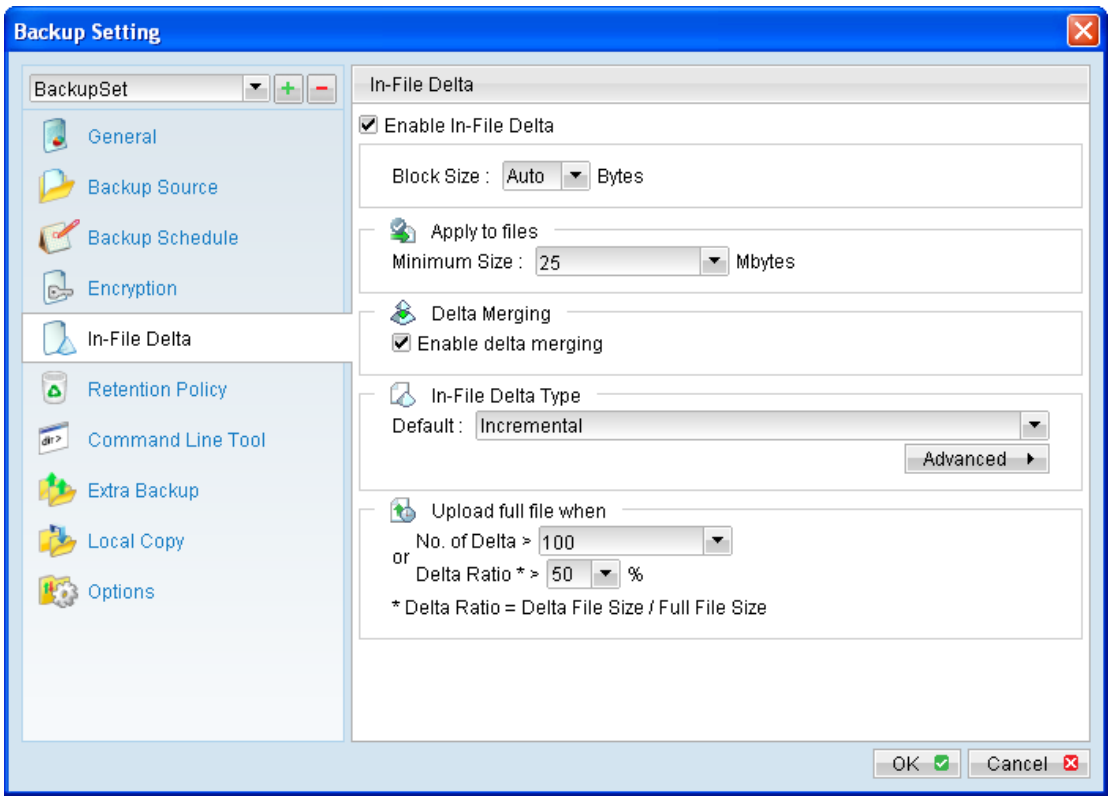
Differential In-File Delta
All differential delta files are generated with respect to changes made since the last full backup file. This means that only the last full backup file and the last differential delta file are required to restore the latest snapshot of a backup file. The other intermediate differential delta files are only required if you want to restore intermediate snapshots of a backup file.

The advantage of a differential In-File delta backup is that a corrupted differential delta file would only make one particular snapshot of a backup file non-recoverable. All other snapshots can still be recovered using the remaining differential delta files.

The full backup file, its checksum file and the last delta file uploaded (if more than one delta files have been uploaded to the backup server) is always stored in the data area. This means that these files are not affected by the setting of the retention policy and will always be kept on the backup server. It is done this way because all these files are required to get the latest snapshot of the backup file and they should not be removed from the backup server by the retention area cleanup routine. All other intermediate delta files are stored in the retention area.

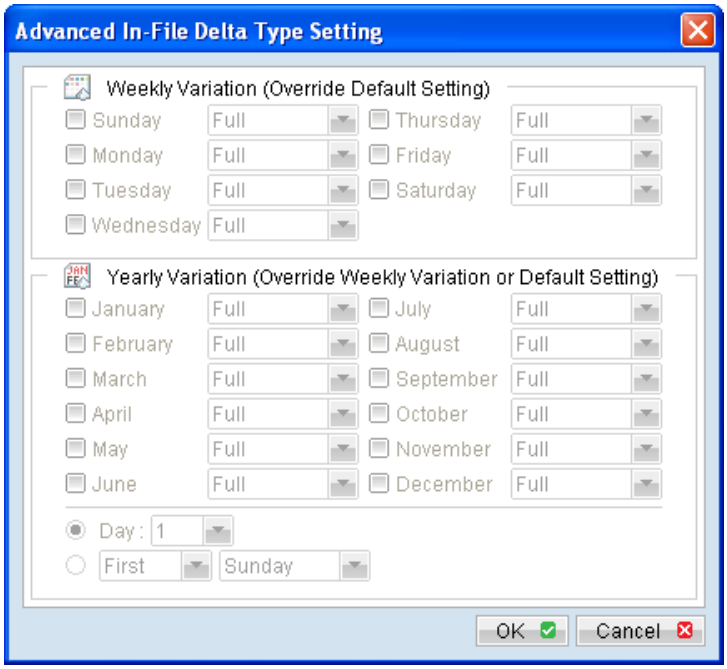
9.1.1.4 Advance In-file Delta Type

[Advanced In-file Delta Type] defines an advance policy, where users can override the default In-file delta setting on specific days in terms of day of a week, or day of a year, for example all Sundays, or the first day of each month.



This is especially useful for users who want to limit their backup on specific day. For example, incremental delta backup on weekdays and differential delta backup on Saturday.

Press the [Advanced] button and the [Advanced In-File Delta Type Setting] dialog will be display.



Menu Items	Description

Weekly Variation (Sunday to Saturday)	Click on the checkbox beside the corresponding day to enable advance In-file delta setting for that day.
Delta type drop down menu (Sunday to Saturday)	Click on the dropdown menu beside the corresponding day to select the delta type for that day.
Yearly Variation (January to December)	Click on the checkbox beside the corresponding day to enable advance In-file delta setting for that day.
Day number (used with yearly variation)	Click on the radio button and dropdown menu to select the day number, of month selected.
Day of week (used with yearly variation)	Click on the radio button and dropdown menus to select the day of week, of the month selected.

9.1.5 Upload full file when

[Upload full file when] defines the rules which OBM will perform a full file backup instead of a delta backup.

OBM will upload a full file when one of the following rules is true:

- When the number of delta files generated (since the last full backup) since the last full file exceeded the [No. of Delta] setting.
- When the delta ratio of the delta file (ratio of delta file size against the full file size) exceeded the [Delta Ratio] setting.

9.1.1.5 No. of Delta

[No. of delta] defines the maximum number of deltas allowed for each full file (within the backup set) before OBM will force a full file upload to the backup server.

For example, if the [No. of delta] is set to 10, and the corresponding file already has 10 deltas saved on the backup server. On the next backup, OBM would upload the full file instead of generating a delta since the [No. of delta] is reached.

This setting is to ensure that there will be a full file backup after a certain number of deltas has been generated (limiting the size of the delta chain).

9.1.2.5 Delta Ratio

[Delta Ratio] defines the maximum 'ratio of change' (delta file size when compare to the last backup) before OBM will force a full file upload to the backup server.

Delta ratio is calculated by dividing the file size of a delta by the file size of the full file (e.g. the percentage of changes detected between the last full backup file and the current file).

For example, if the [Delta Ratio] is set to 50% (default setting), if a file changes by more than 50%, OBM would upload the full file instead of generating a delta since the [Delta Ratio] is reached.

This setting is to ensure that a full file backup is performed for file with significant changes, as it is preferable to upload a full file instead to reduce the time required to restore the file.

10 Backup / Restore Windows System State

This chapter describes in details how to backup and restore Windows System State with OBM.

10.1 Supported versions

The System State backup module is supported for the following Windows platforms:

- Windows XP
- Windows Server 2003 / R2
- Windows Server 2008 / R2
- Windows Small Business Server 2011

10.2 Requirements and recommendations

For System State backup of **Windows XP or 2003 / R2**, please ensure that the following requirements or recommendations are met:

1. OBM is installed on the computer to be backed up.
2. Sufficient disk spaces are required for the temporary directory (usually of size around 2 GB).
3. It is recommended that the temporary directory be configured on a local drive.

For System State backup of **Windows 2008 / R2 or SBS 2011**, please ensure that the following requirements or recommendations are met:

1. OBM version 6.3 or above is installed on the computer to be backed up.
2. The system volume must be formatted with NTFS.
3. Sufficient disk spaces are required for the temporary directory (usually of size around 10 GB).
4. The following Windows Features are installed on the client computer (under Server Manager):
    - Windows Server Backup Features
        - Windows Server Backup
        - Command line Tool
    - Windows PowerShell

5. Limitations on the temporary directory:

   - Temporary directory must be a local or USB drive.
   - Temporary directory can be a non-critical or critical drive.
   - Temporary directory can only be set to the root of a drive.
   - Shadow Copies storage location of temporary directory must be set to local.

   Please refer to the following Help Centre article for details.
   https://help..com/openArticle.aspx?aid=2869

6. It is recommended that the temporary directory be configured on a local drive

10.3 Overview

The following steps are performed during a backup job:

1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Commands are issued to create the System State data:

   - Windows XP, 2003 (*Ntbackup*)
   - Windows Server 2008, SBS 2011 (*Wbadmin*)

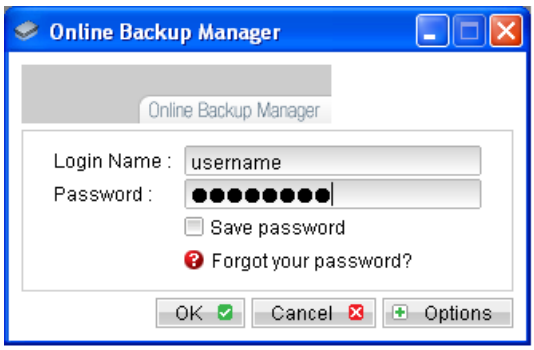
4. System State data is temporarily stored in the temporary directory specified in the backup set.
5. Server and local file lists are compared to determine which file will be uploaded
6. Delta file is generated for modified file (if necessary).
7. Data are encrypted, compressed, and uploaded to the backup server.
8. System State data is removed from the temporary directory specified in the backup set.
9. Backup completed successfully.

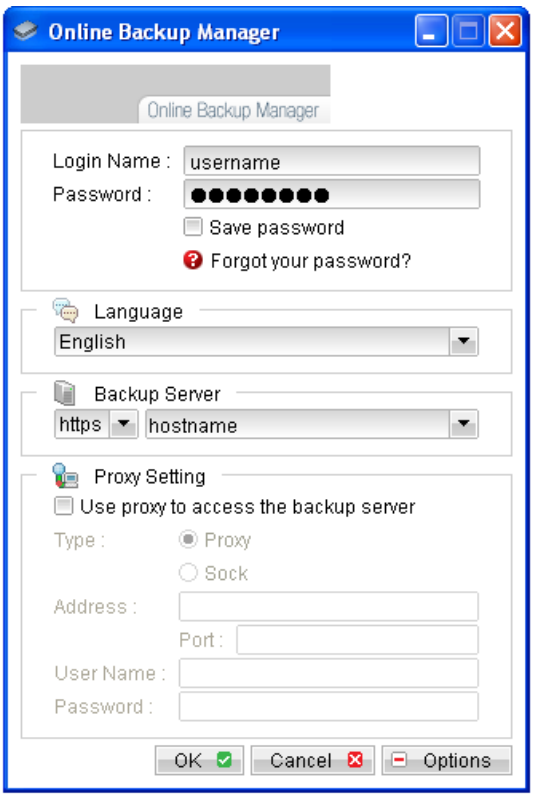
10.4 How to backup Windows System State

Refer to the following instructions to backup Windows System State:

10.4.1 For Windows XP, 2003 / R2

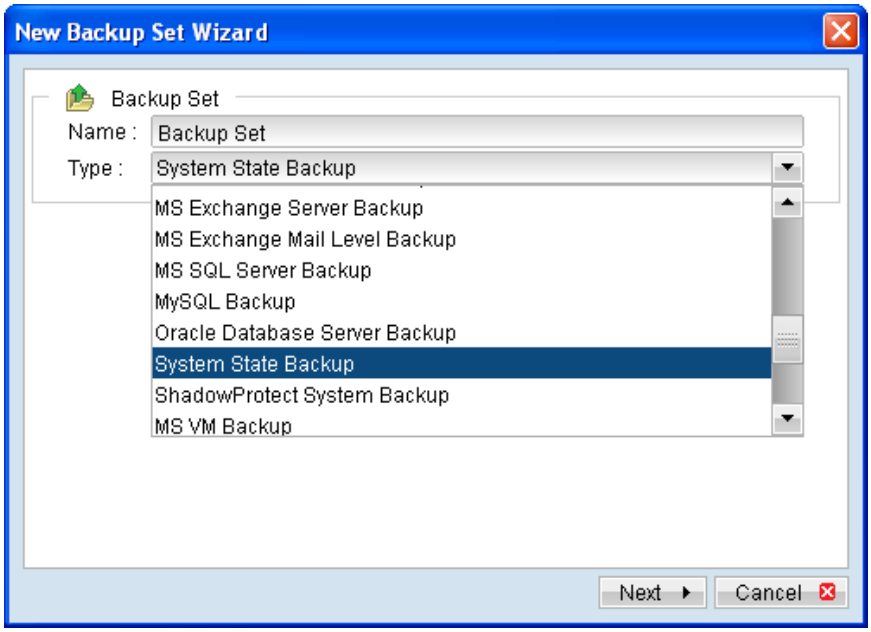
1. Login to the backup application's user interface.





2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

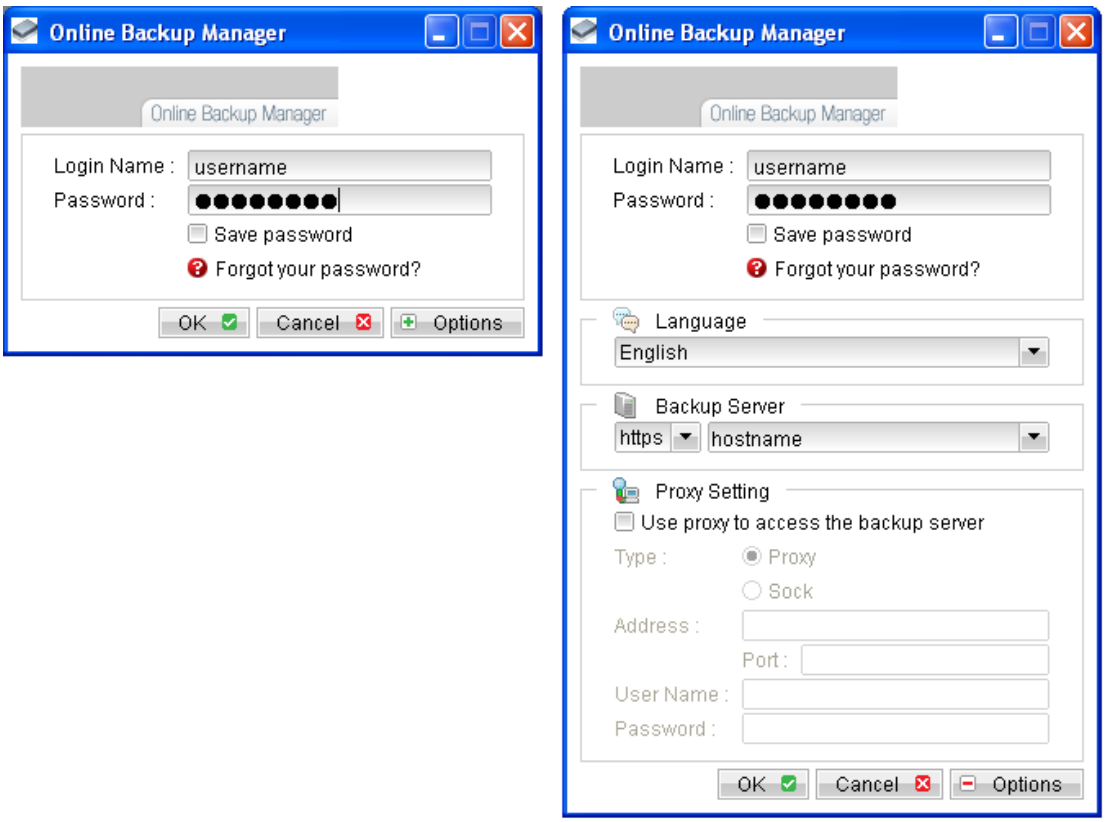
3. Create a System State Backup set by selecting [System State Backup] from the backup set type dropdown menu.



4. Select [Next] to proceed.
5. Configure a backup schedule for unattended backups.
6. Select an encryption setting for your backup set.
7. Press the [OK] button to complete the configuration of backup set.
8. Scheduled backup will run automatically at the configured schedule time.
9. Click [Backup] button on the left panel to perform a backup immediately.

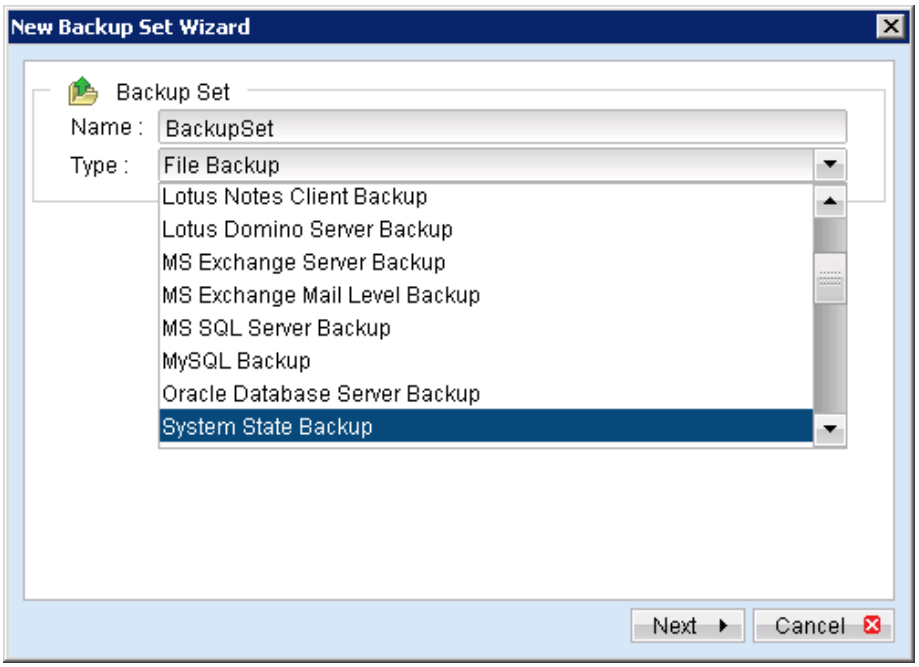
10.4.2 For Windows Server 2008 / R2, SBS 2011

1. Login to the backup application's user interface.



2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

3. Create a System State Backup set by selecting [System State Backup] from the backup set type dropdown menu.



4. Select [Next] to proceed.

5. Configure a backup schedule for unattended backups.

   Note:
   Multiple backup schedules of different types can be configured for the same backup set.

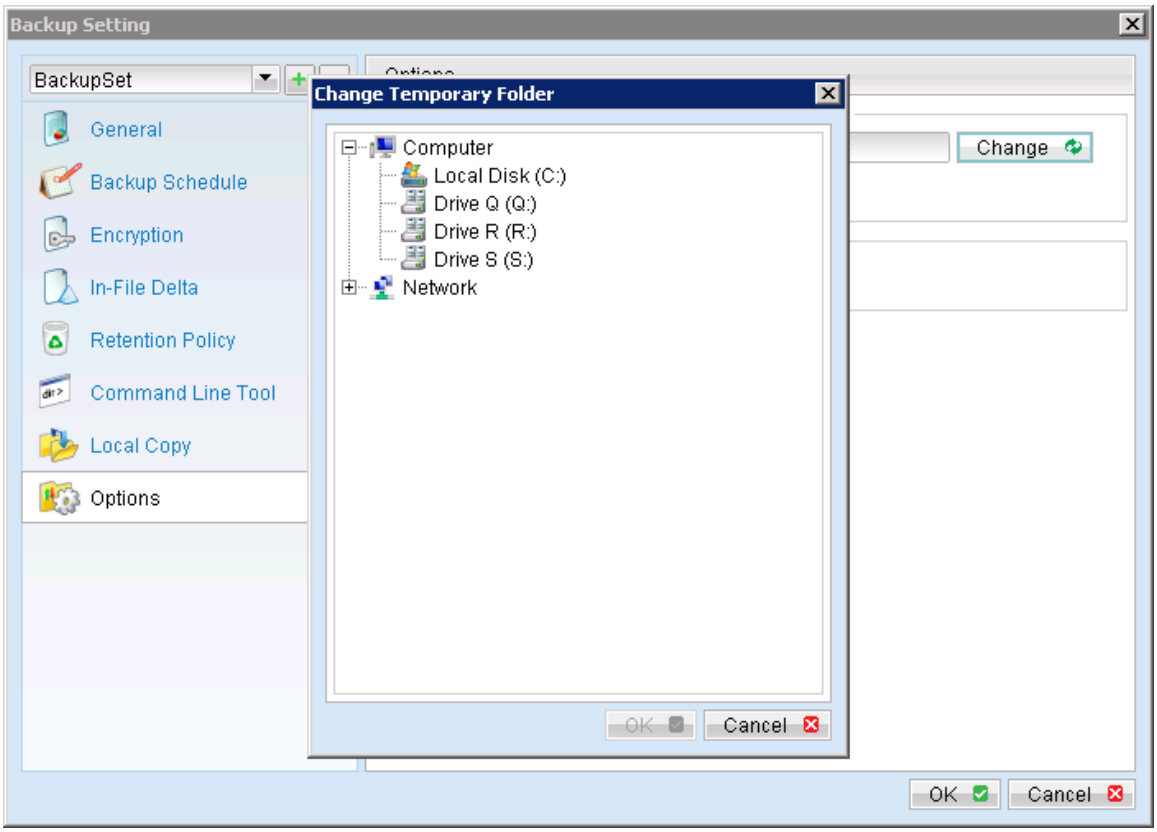
6. Select an encryption setting for your backup set.

7. Press the [OK] button to complete the configuration of backup set.

8. Configure the temporary directory of the System State backup set.

9. On the OBM main menu, press [Backup Setting], then [Options].

10. Click [Change] and select the temporary volume for backup.



11. Scheduled backup will run automatically at the configured schedule time.

12. Click [Backup] button on the left panel to perform a backup immediately.

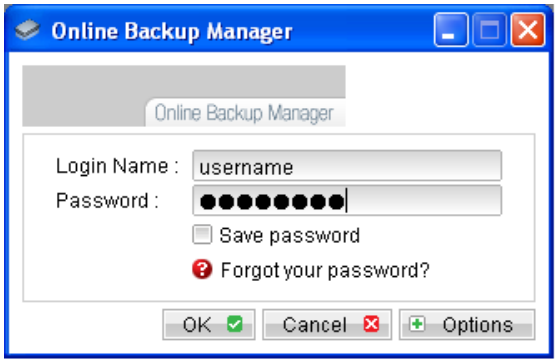
10.5 How to restore Windows System State

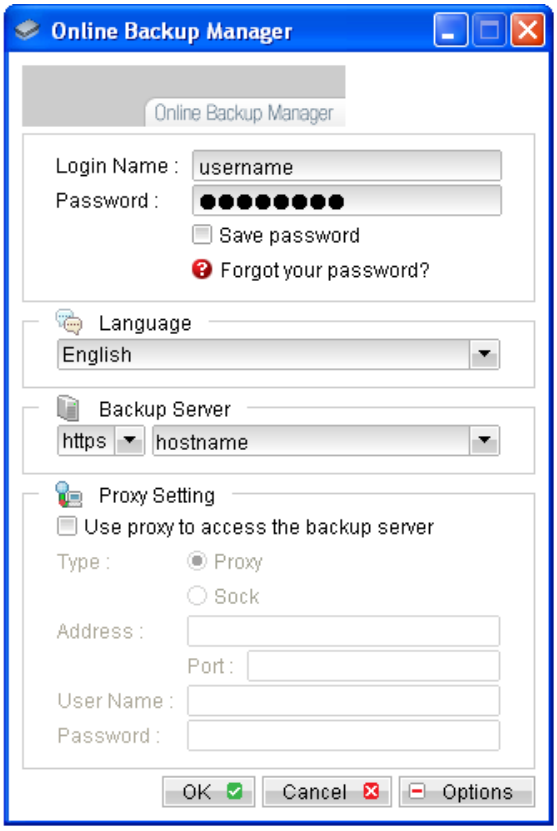
10.5.1 For Windows XP, 2003 / R2

Refer to the following instructions to restore Windows System State on Windows XP, Server 2003 / R2:

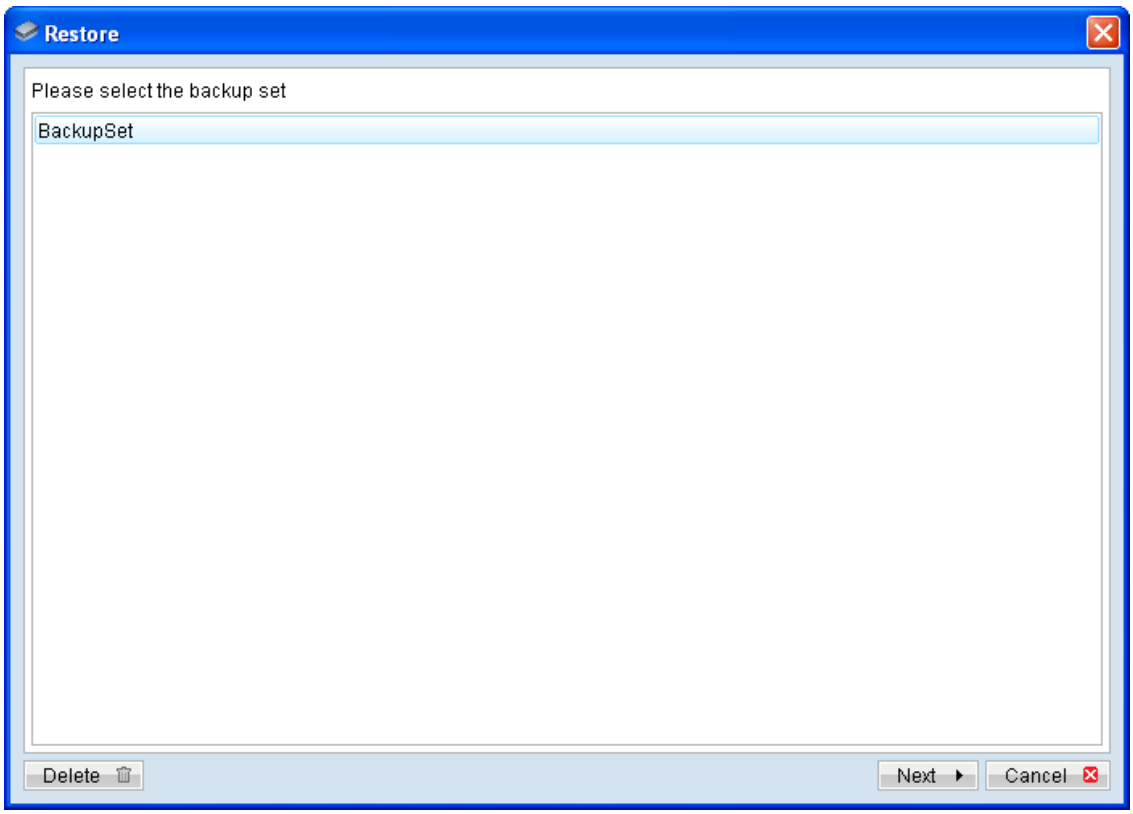
1. Install OBM on the machine to be restored to.

2. Login to the backup application's user interface.

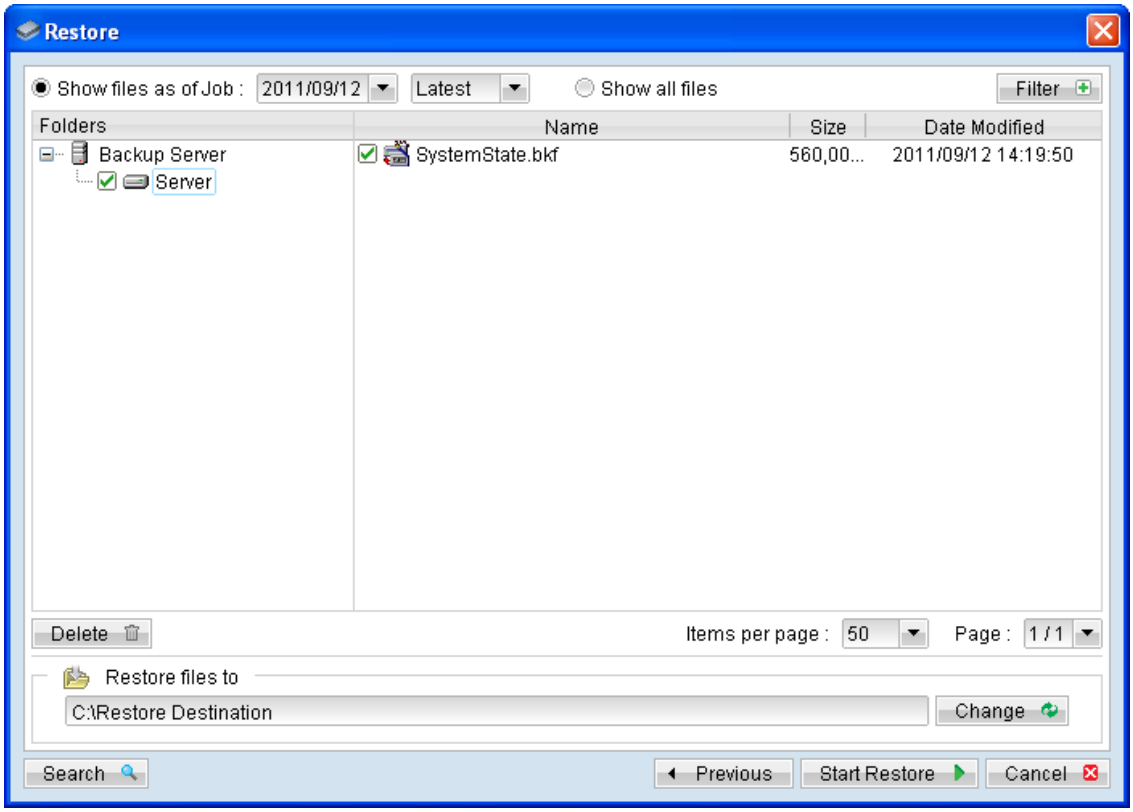




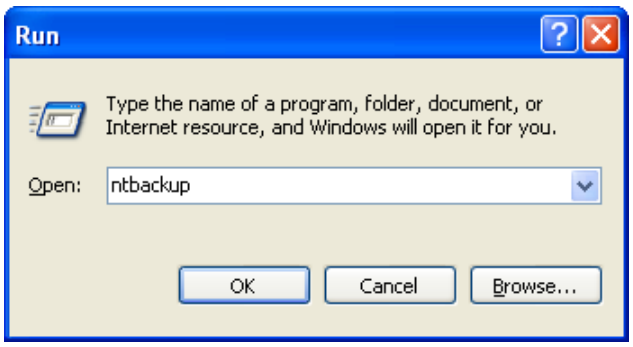
3. Select the [Restore] button and the corresponding backup set.



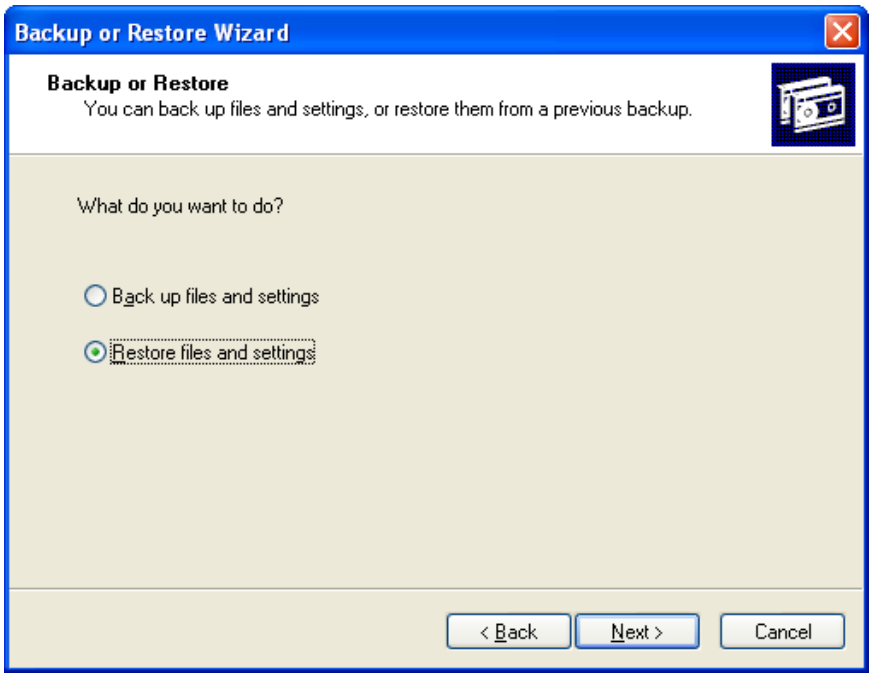
4. Select the System State file (SystemState.bkf) to be restored and its restore destination.



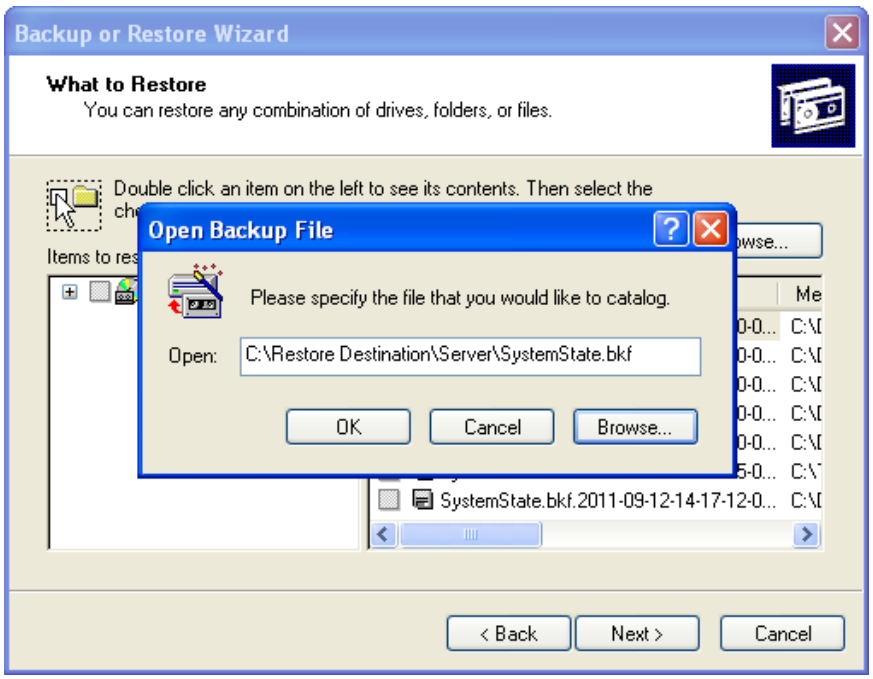
5. Open NTBackup, in the Windows Start menu, click [Run…] and type in ntbackup.



6. Press [Next] and select [Restore files and settings]

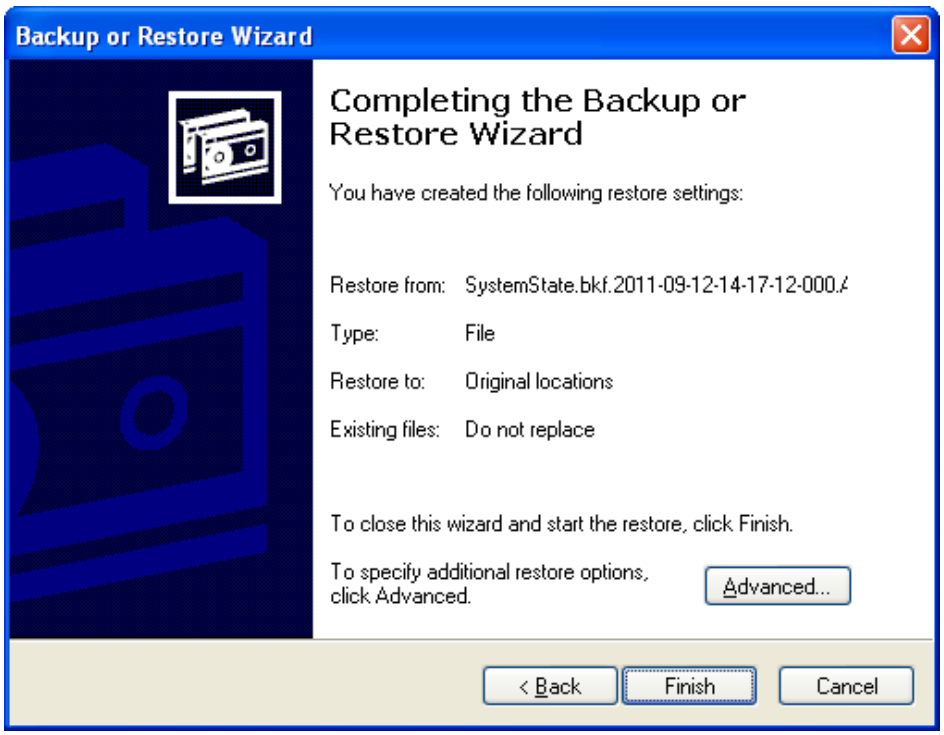

Backup or Restore Wizard
Backup or Restore
You can back up files and settings, or restore them from a previous backup.
What do you want to do?
Back up files and settings
Restore files and settings
< Back
Next >
Cancel

7. Click [Browse], browse to the SystemState.bkf file which you have restored via OBM, then press [OK].



8. Expand and select the corresponding System State file from the left panel, press [Next] afterward.

9. Review the settings then press [Finish] to begin the restore process.


Backup or Restore Wizard
Completing the Backup or Restore Wizard
You have created the following restore settings:
Restore from: SystemState.bkf.2011-09-12-14-17-12-000.
Type: File
Restore to: Original locations
Existing files: Do not replace
To close this wizard and start the restore, click Finish.
To specify additional restore options, click Advanced.
Advanced...
< Back
Finish
Cancel

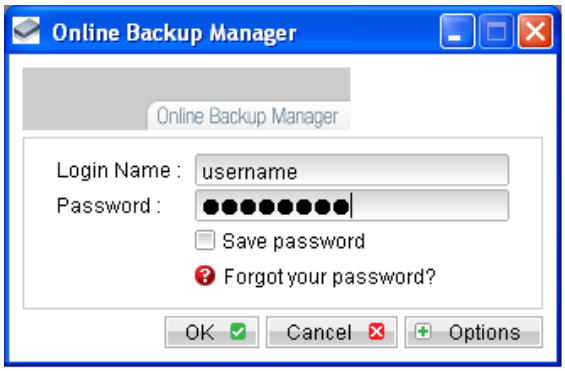
10. The restore process is now completed.

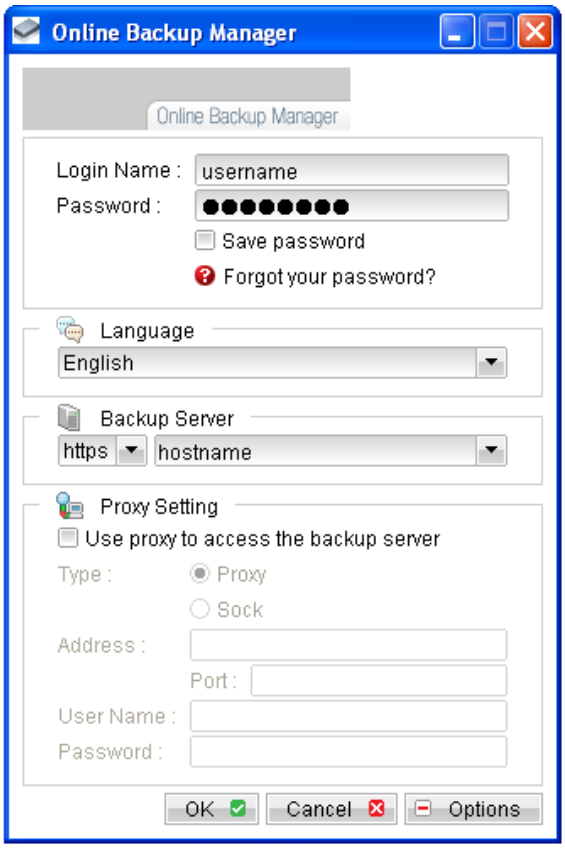
10.5.2 For Windows 2008 / R2, SBS 2011

Refer to the following instructions to restore Windows System State on Windows Server 2008 / R2, SBS 2011:

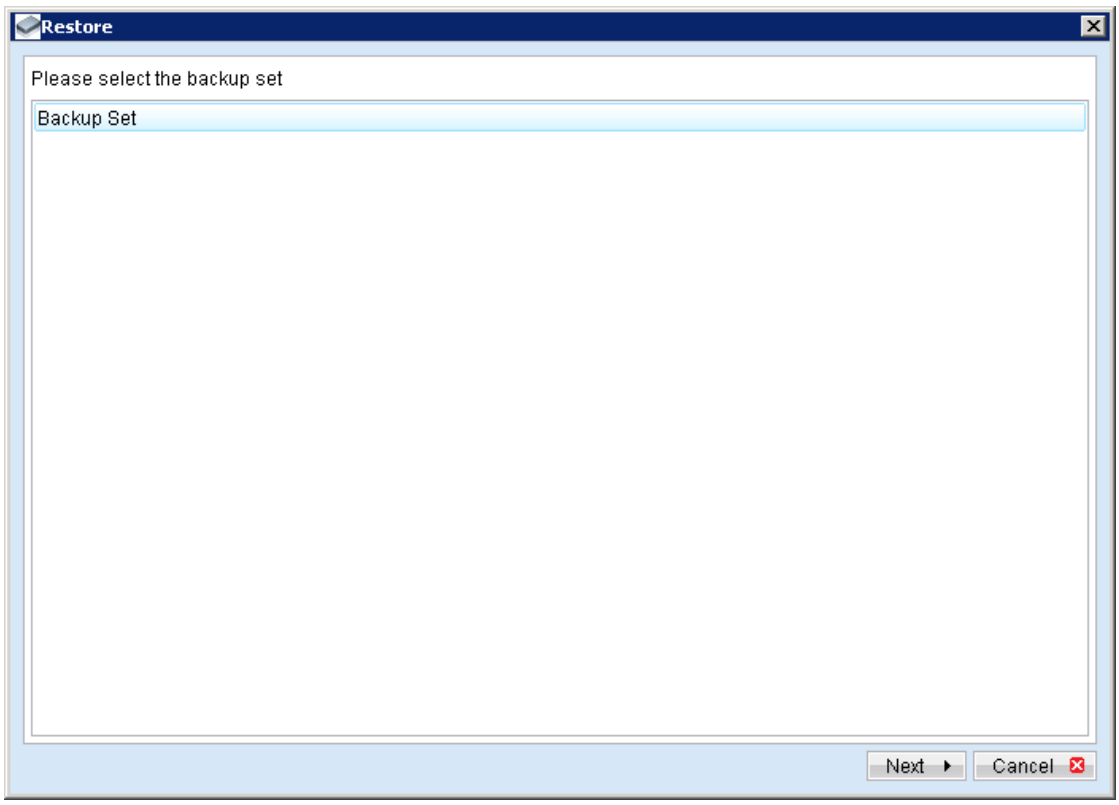
1. Install OBM on the machine to be restored to.

2. Login to the backup application's user interface.

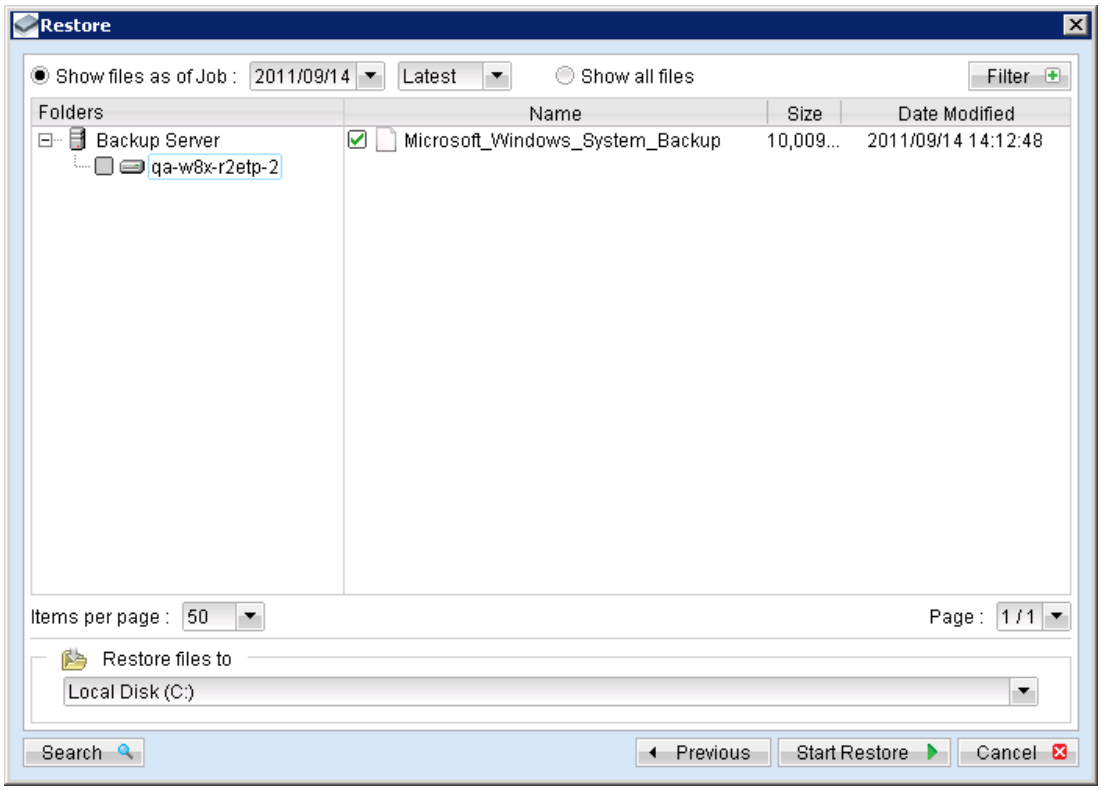




3. Select the [Restore] button and the corresponding backup set.



4. Select the System State file to be restored and its restore destination.



5. Insert the Windows Setup Disc into the CD / DVD drive

6. Restart the computer. In some case, you need to press the required key to boot up the server from disc; the [Install Windows Wizard] should appear.

7. Specify the language settings, and then click [Next].

8. Click [Repair your computer].

9. Setup will search the hard disk drives for existing Windows installation, then displays the result in [System Recovery Options].

   If you are recovering the operating system onto a new hardware setup, the list will be empty (e.g. there is no existing operating system).

   Click [Next] afterward.

10. On the [System Recovery Options] page, click [Windows Complete PC Restore]. This opens the Windows Complete PC Restore Wizard.

11. Select one of the following options then click [Next]:

    - Click [Use the latest available backup (recommended)].

    - Click [Restore a different backup].

12. For [Restore a different backup], select one of the following option on [Select the location of the backup] then click [Next]:

    - Click the computer that contains the backup that you want to use.

    - Under [Select the backup to restore], click the backup to be used.

    - Click [Advanced] to browse for a backup on the network.

13. On the [Choose how to restore the backup] page, perform the following optional tasks, and then click [Next]:

    - Select the [Format and repartition disks] check box to delete existing partitions and reformat the destination disks to be the same as the backup.

      This enables the [Exclude disks] button. Click this button and then select the check boxes associated with any disks that you want to exclude from being formatted and partitioned.

      The disk that contains the backup that you are using is automatically excluded.

      Note:
      Unless a disk is excluded, data on it can be lost, regardless of whether it was part of the backup or whether it has volumes that are being restored.

- Select the [Only restore system disk] check box to perform an operating system only recovery.
- Click [Install drivers] to install drivers for the hardware that you are recovering to.
- Click [Advanced] to specify whether the computer is restarted and the disks are checked for errors immediately after the recovery.

14. Confirm the details for the restoration, and then click [Finish].

10.5.3 For Windows 2008 / R2 Domain Controller

Refer to the following instructions to restore Windows System State on Windows Server 2008 / R2 Domain Controller:

Important:
Authoritative restore of Windows 2008 Domain Controller is required only if you need to restore deleted Active Directories objects.

Please follow the instructions below to restore a system state backup to a Windows 2008 Domain Controller:

1. Reboot the Windows Server 2008 / R2 Domain Controller in Directory Service Repair Mode (DSRM):
   - Add the safeboot option to the default boot loader. In command prompt, type in the following command:

```
>bcdedit /set safeboot disrepair
```

   - Reboot the computer.

2. Perform the restore on the Domain Controller:
   - Open command prompt and type the following:

```
>wbadmin get versions
```

   This will list all the known backups available.
   - Type the following command to perform an authoritative restore:

```
```

```
>wbadmin start systemstaterecovery –
version:<backup_version> -authsysvol
```

For non-authoritative restore, please type the following command:

```
>wbadmin start systemstaterecovery –
version:<backup_version> -authsysvol
```

Backup version is the identifier of one of the backup snapshots listed in previous step.

3. Reboot the Windows Server 2008 / R2 Domain Controller in Normal Mode:

   - Remove the safeboot option to the default boot loader. In command prompt, type in the following command:

```
>Bcdedit /deletevalue safeboot
```

   - Reboot the computer.

4. The restore process is now completed.

11 Backup / Restore Windows System (WBAdmin)

This chapter describes in details how to backup and restore Windows System with OBM (MS Windows System backup Module).

11.1 Supported versions

The MS System backup module is supported for the following Windows platforms:

- Windows Vista*
- Windows 7*
- Windows Server 2008 / R2
- Windows Small Business Server 2011

* All except Home Edition.

11.2 Requirements and recommendations

Please ensure that the following requirements or recommendations are met by the backup client computer:

1. OBM is installed on the computer to be backed up.

2. Sufficient disk spaces are required for the temporary storage volume of the System backup.

   It is recommended to have free disk space of 150% x Total In-use Size of all volumes selected for backup.

3. The following Windows Features are installed on the client computer:

   - Windows Server Backup Features

     - Windows Server Backup
     - Command line Tool
     - Windows PowerShell

4. Limitations on the temporary directory:

   Please refer to the following Help Centre article for details.

   https://help..com/openArticle.aspx?aid=2869

5. It is recommended that the temporary directory be configured on a local drive.

11.3 Overview

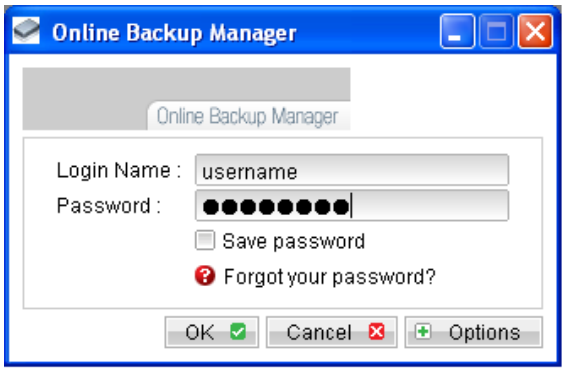
The following steps are performed during a backup job:

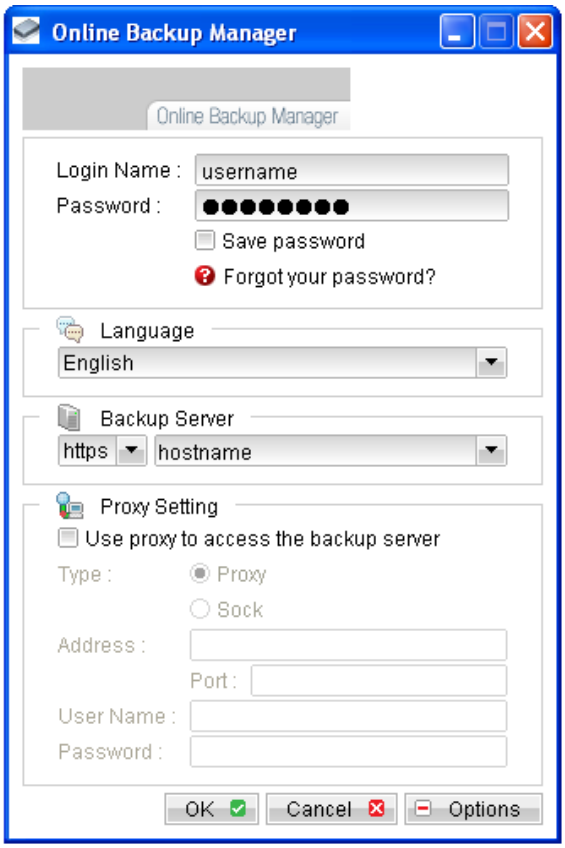
1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Commands are issued to create the System backup data.
4. System backup data is temporarily stored in the temporary storage volume in the backup set.
5. System backup data are compressed into 1 single file.
6. Server and local file lists are compared to determine which file will be uploaded.
7. Delta file is generated (if necessary).
8. Data is encrypted, and uploaded to the backup server.
9. System backup data is removed from the temporary storage volume specified in the backup set.
10. Backup completed successfully.

11.4 How to backup Microsoft Windows System (WBAdmin)

Refer to the following instructions to backup Windows System:

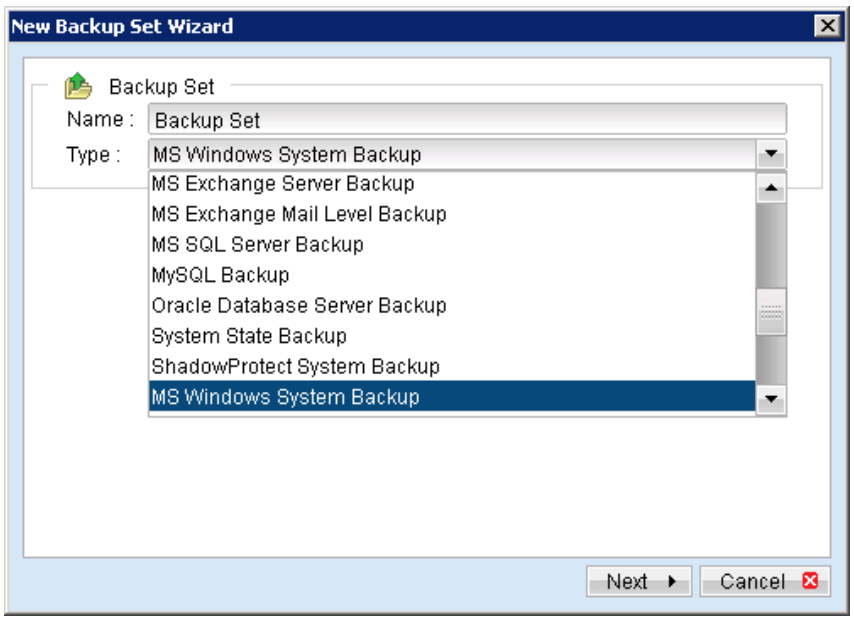
1. Login to the backup application's user interface.





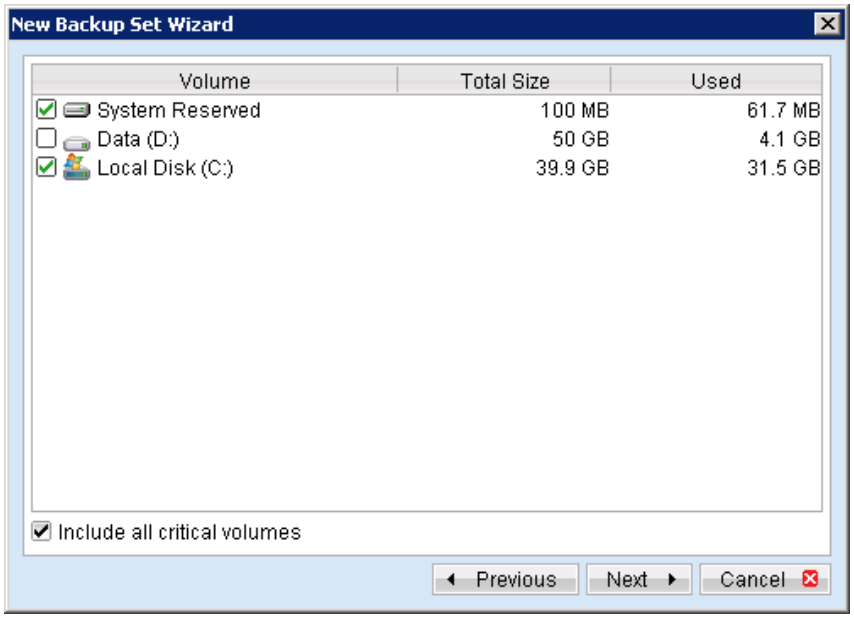
2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

3. Create a MS Windows System Backup set by selecting [MS Windows System Backup] from the backup set type dropdown menu.



4. Select [Next] to proceed.

5. Select the corresponding volumes for backup.



Important:
For complete backup of the system, it is recommended to select the [Include all critical volumes] option.

This will automatically includes the system partition, boot partition, system reserved partition and other partitions that contain critical system data.

6. Configure a backup schedule for unattended backups.

Note:

Multiple backup schedules of different types can be configured for the same backup set.

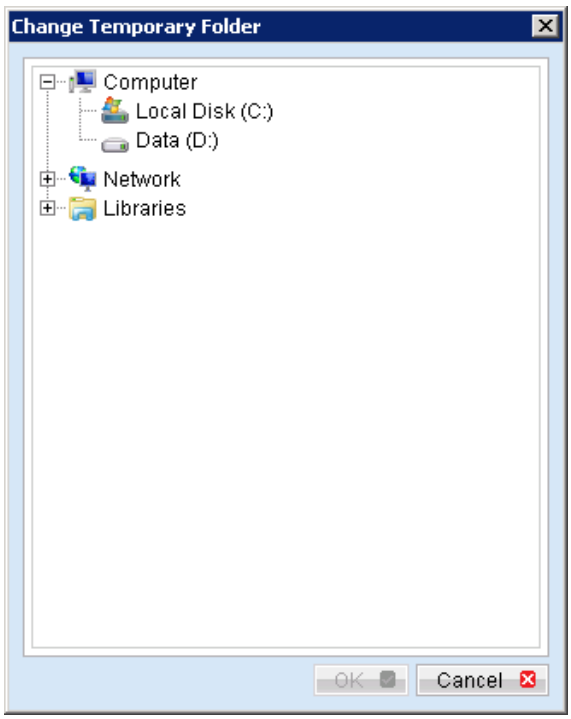
7. Select an encryption setting for your backup set.

8. Press the [OK] button to complete the configuration of backup set.

9. Configure the temporary directory of the MS Windows System backup set.

10. On the OBM main menu, press [Backup Setting], then [Options].

11. Click [Change] and select the temporary volume for backup.



12. Scheduled backup will run automatically at the configured schedule time.

13. Click [Backup] button on the left panel to perform a backup immediately.

11.5 How to restore Microsoft Windows System (WBAdmin)

Refer to the following instructions to restore a Windows System:

There are several methods which you can restore the Windows System

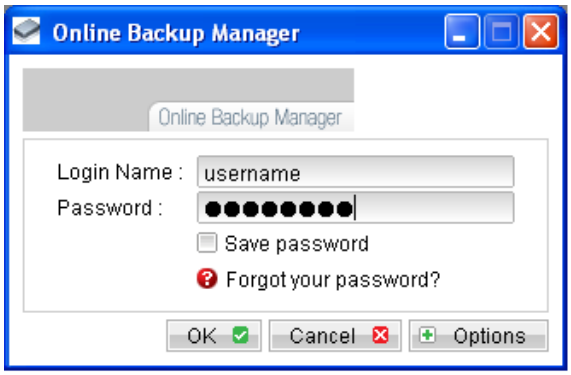
- Recover volumes with the Recovery Wizard
- Recover the operating system with the Install Windows Wizard
- Recover volumes with command
- Recover with the Windows Recovery Environment

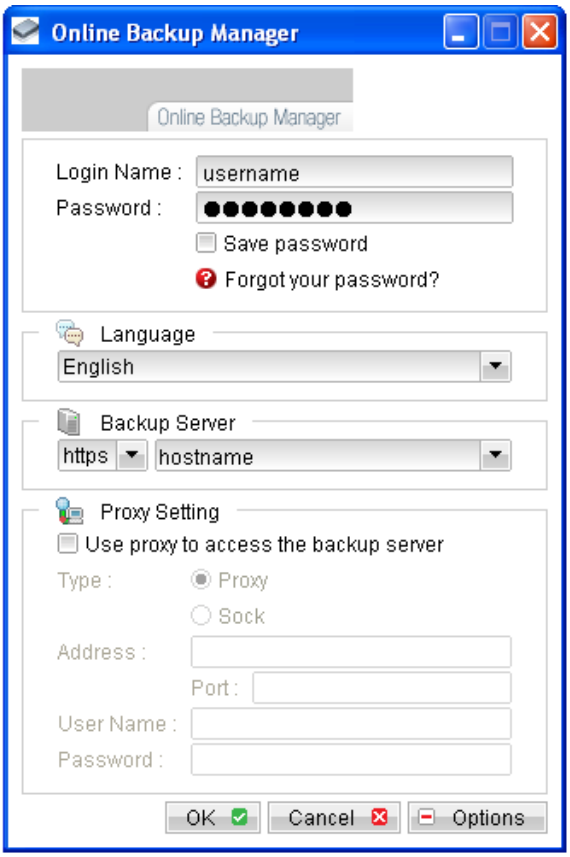
Important:
The volume to be recovered to must be the same size or larger than the volume that was backed up from.

Restore the system data from the OBS server:

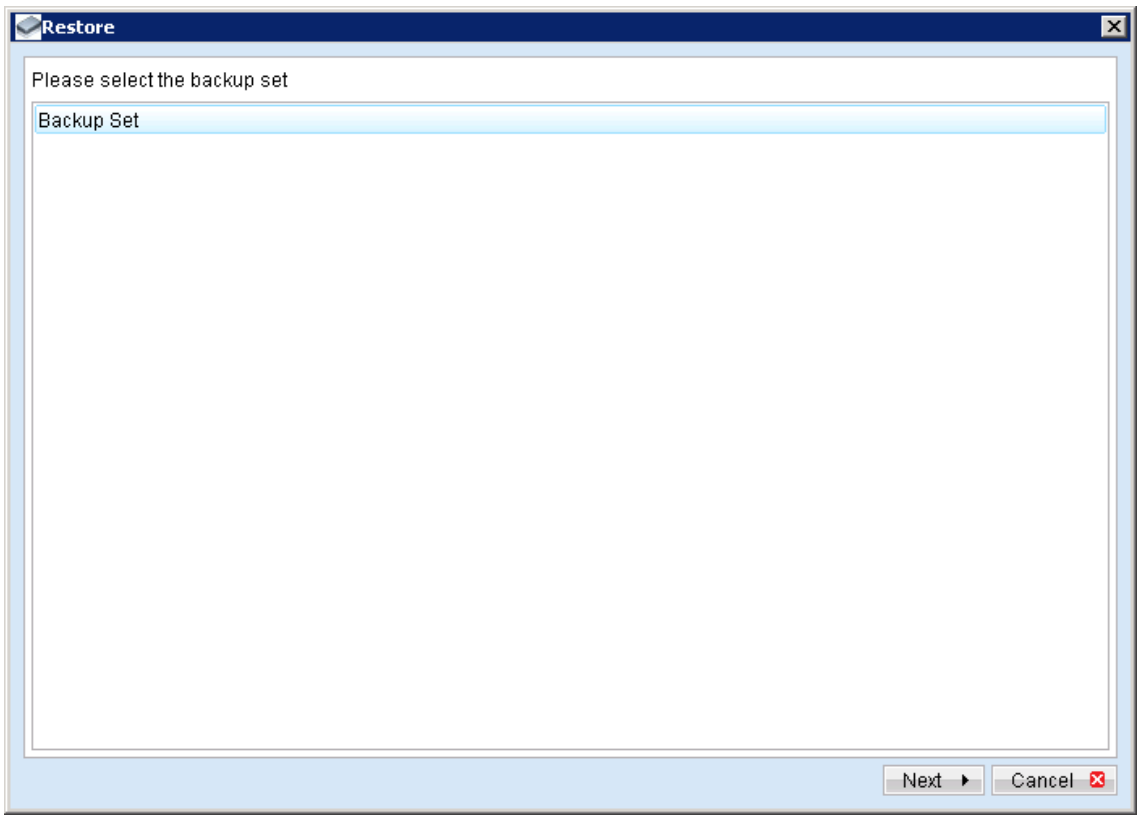
1. Install OBM on the machine to be restored to.

2. Login to the backup application's user interface.

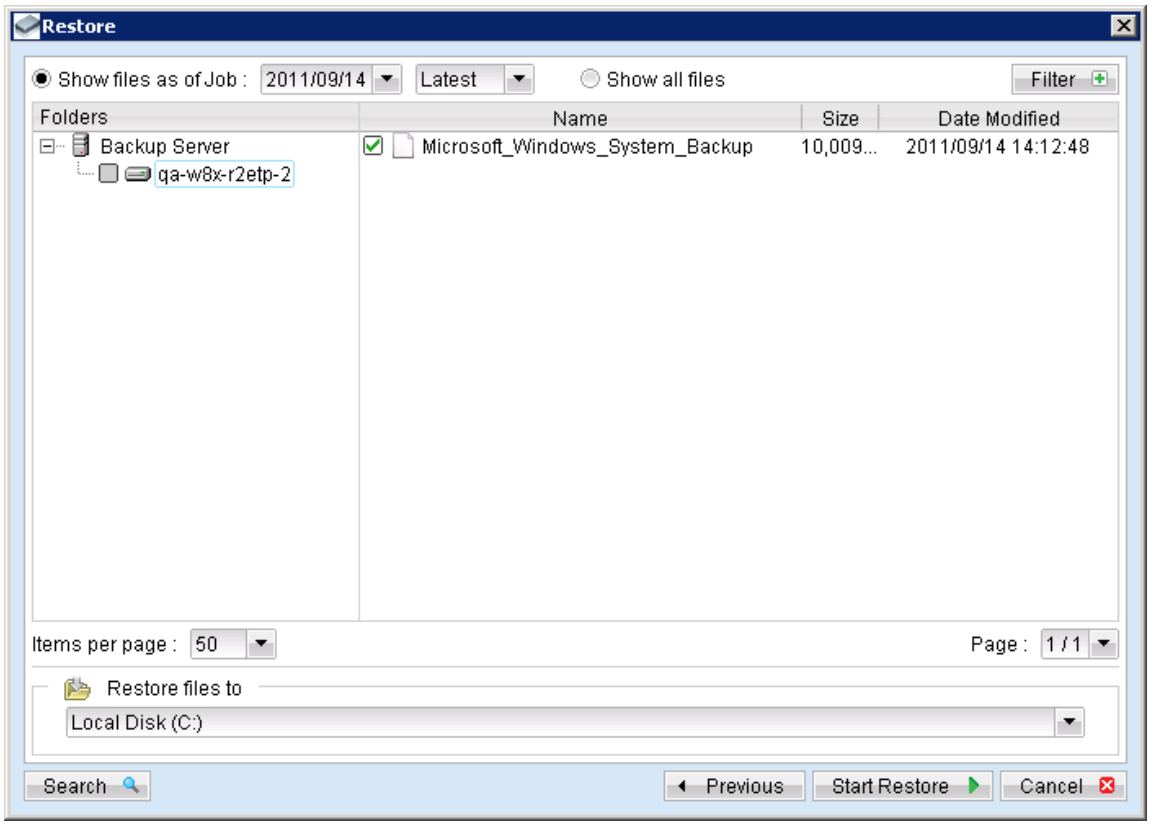




3. Select the [Restore] button and the corresponding backup set.



4. Select the system file to be restored and its restore destination.



5. Continue to the next sections for instructions to restore the Windows System.

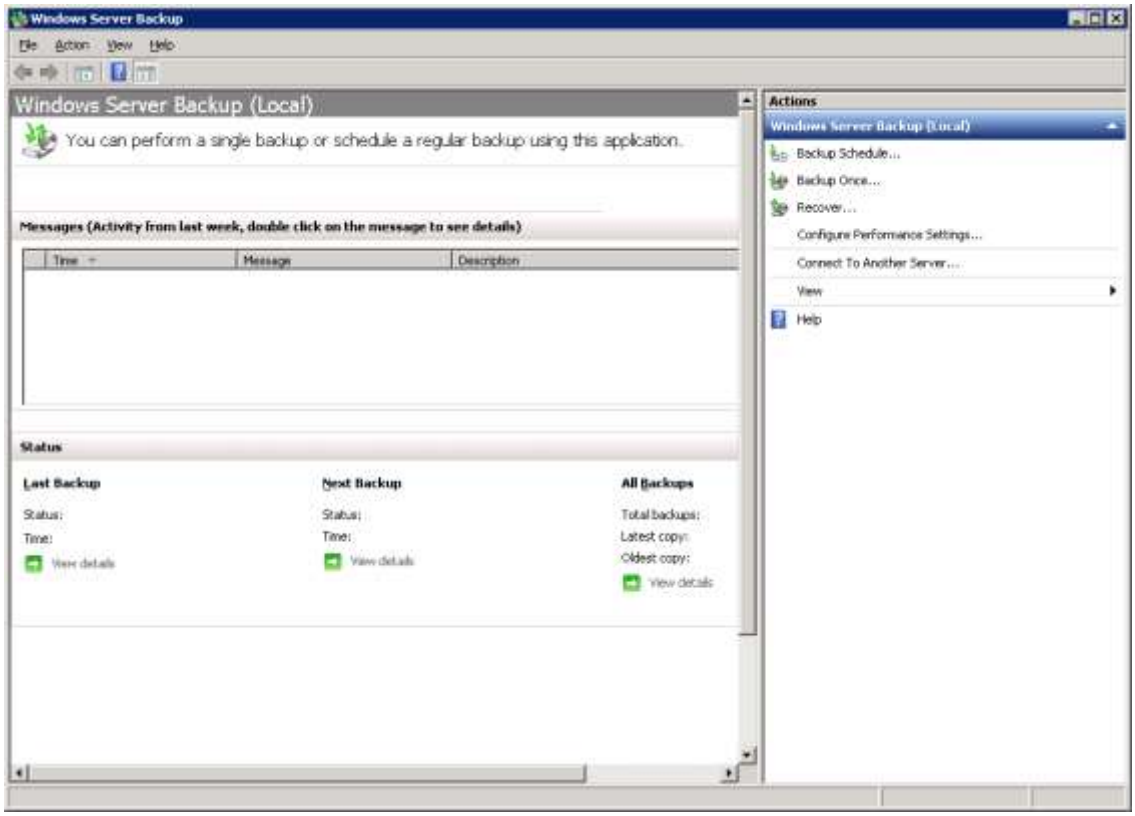
Important:
Before continuing, the Windows account which you are using must be a member of the Backup Operators or Administrators group.

11.5.1 Recover volumes with the Recovery Wizard

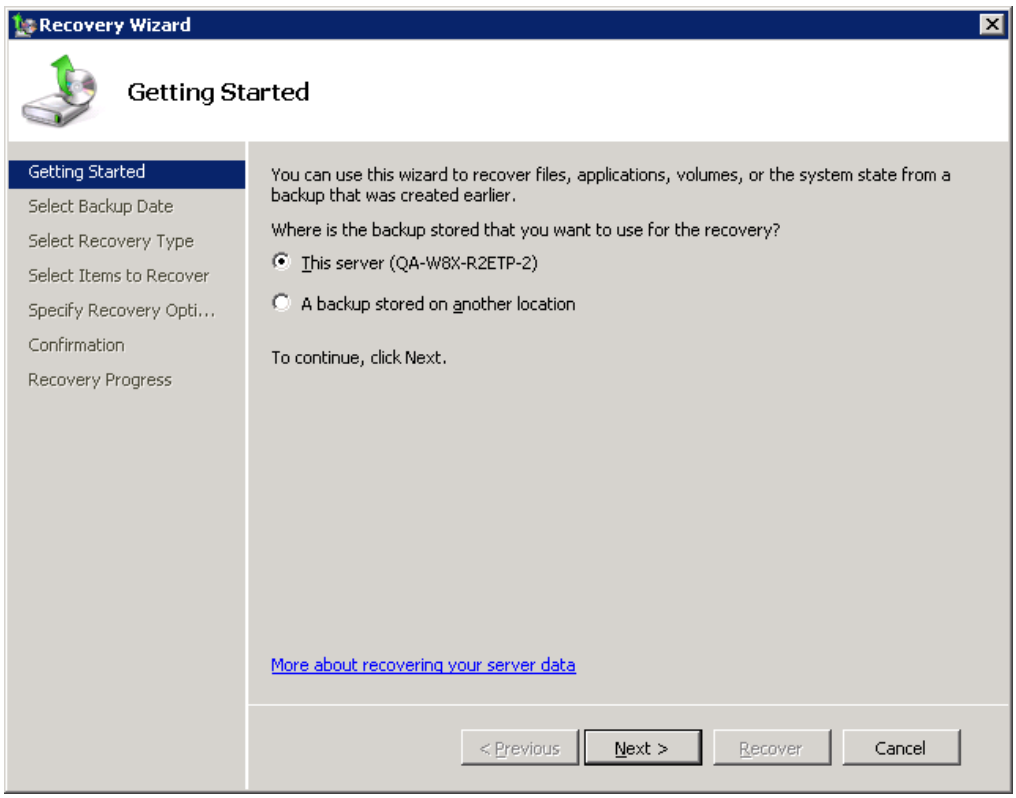
Refer to the following instruction to perform a volume recovery with the Recovery Wizard:

1. From the [Start] menu, click [Administrative Tools], and then click [Windows Server Backup].

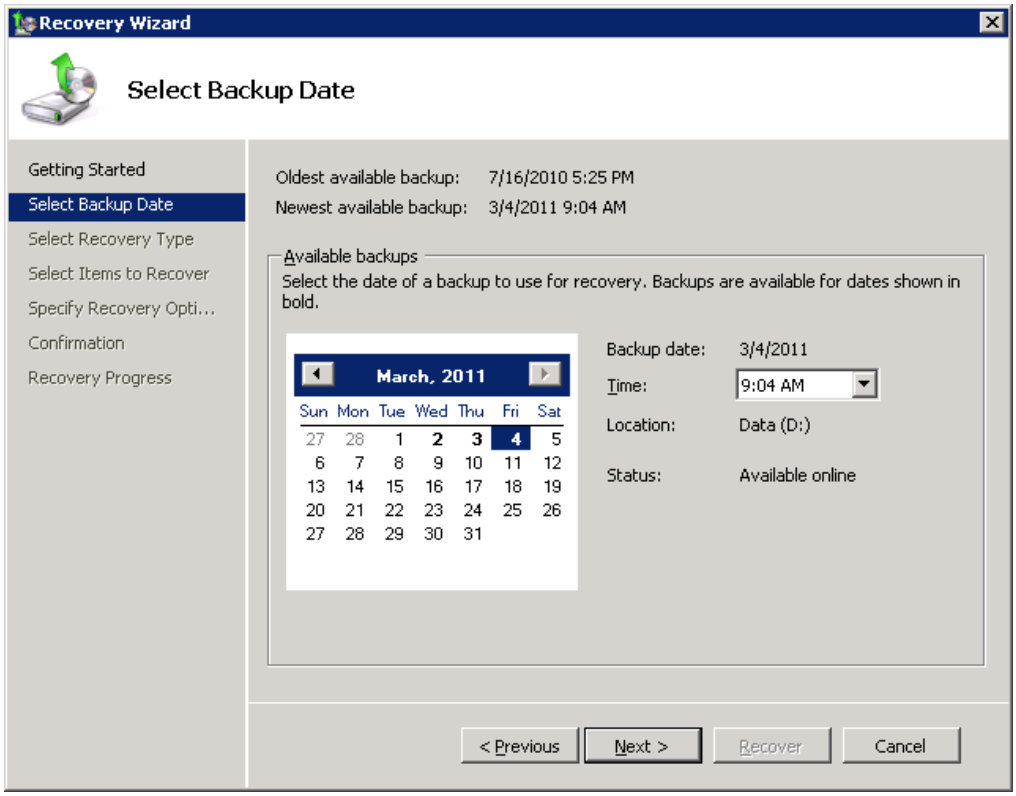
2. In the [Actions] panel under [Windows Server Backup], click [Recover] to open the Recovery Wizard.



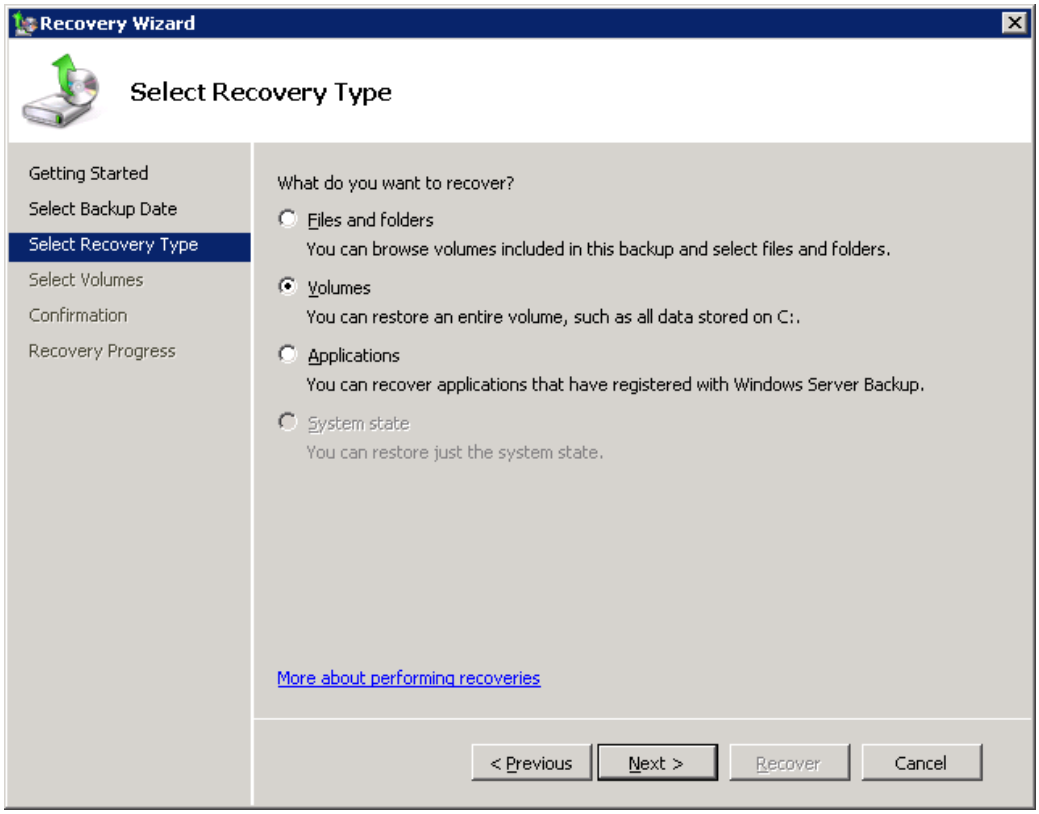
3. In the [Getting Started] menu, specify the backup is stored on [This server], click [Next].


Recovery Wizard
Getting Started
Getting Started
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Opti...
Confirmation
Recovery Progress
You can use this wizard to recover files, applications, volumes, or the system state from a backup that was created earlier.
Where is the backup stored that you want to use for the recovery?
This server (QA-W8X-R2ETP-2)
A backup stored on another location
To continue, click Next.
More about recovering your server data
< Previous
Next >
Recover
Cancel

4. In the [Select Backup Date] menu, select the date from the calendar and the time from the drop-down list of backup to restore from.


Recovery Wizard
Select Backup Date
Getting Started
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Opti...
Confirmation
Recovery Progress
Oldest available backup: 7/16/2010 5:25 PM
Newest available backup: 3/4/2011 9:04 AM
Available backups
Select the date of a backup to use for recovery. Backups are available for dates shown in bold.
March, 2011
Sun Mon Tue Wed Thu Fri Sat
27 28 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31
Backup date: 3/4/2011
Time: 9:04 AM
Location: Data (D:)
Status: Available online
< Previous
Next >
Recover
Cancel

5. In the [Select Recovery Type] menu, click [Volumes], and then click [Next].


Recovery Wizard
Select Recovery Type
Getting Started
Select Backup Date
Select Recovery Type
Select Volumes
Confirmation
Recovery Progress
What do you want to recover?
Files and folders
You can browse volumes included in this backup and select files and folders.
Volumes
You can restore an entire volume, such as all data stored on C:.
Applications
You can recover applications that have registered with Windows Server Backup.
System state
You can restore just the system state.
More about performing recoveries
< Previous
Next >
Recover
Cancel

6. On the [Select Volumes] Menu, select the check boxes associated with the volumes to be recover.

7. From the associated drop-down list in the [Destination Volume] column, select the recovery destination volume, and click [Next].

8. On the [Confirmation] menu, review the details; click [Recover] to begin the restore process.

11.5.2 Recover the operating system with the Install Windows Wizard

Refer to the following instruction to perform an operating system recovery with the Install Windows Wizard:

1. Insert the Windows Setup Disc into the CD / DVD drive.

2. Restart the computer.

   Note:
   In some case, you may need to press the required key to boot up from disc.

3. Specify the language settings, and then click [Next].

Install Windows
Windows Server 2008
Language to install: English
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
Copyright © 2009 Microsoft Corporation. All rights reserved.
Next

4. Click [Repair your computer].

Install Windows
Windows Server 2008
Install now
What to know before installing Windows
Repair your computer
Copyright © 2009 Microsoft Corporation. All rights reserved.

5. Setup will search the hard disk for existing Windows installation, then displays the result in [System Recovery Options].

6. Click [Next] afterward.

7. On the [System Recovery Options] page, click [System Image Recovery].

8. Perform one of the following actions:

   - Click [Use the latest available system image (recommended)] and then click [Next].

   - Click [Select a system image] and then click [Next].

9. If the option [Select a system image] is selected, perform one of the following actions on the [Select the location of the backup] page:

   - Select the volume containing the backup data to be restored and click [Next].

   - On the [Select the date and time of system image to restore] page, select the version to be restored, and then click [Next].

- Click [Advanced] to browse for a backup on the network, and then click [Next].

10. On the [Choose how to restore the backup] page, perform the following optional tasks, and then click [Next]:

    - Select the [Format and repartition disks] check box to delete existing partitions and reformat the destination disks to be the same as the backup.

    - Click the [Exclude disks] button and then the checkbox beside the disk to be excluded from being formatted and partitioned

    - Select the [Only restore system disk] check box to perform an operating system only recovery.

    - Click [Install drivers] to install drivers for the hardware to be recovering to.

    - Click [Advanced] to specify whether the computer is restarted and the disks are checked for errors immediately after the recovery.

11. Click [Finish] to begin the restore process.

11.5.3 Recover volumes with command

Refer to the following instruction to perform a volume recovery with command:

1. Open command prompt.

2. Enter the following command, according to the backup data source, target:

```
>Wbadmin start recovery
 -version:<VersionIdentifiers>
 -itemType:Volume
 -items:<VolumesToRecover>
 -backupTarget:<VolumeHostingBackup>
 -recoveryTarget:<TargetVolumeForRecovery>
```

Parameter	Descriptions
-version	**Specifies the version identifier of the backup to recover in the following format:** **MM/DD/YYYY-hh:mm** **Type in the following to list version identifier:** **>Wbadmin get versions**
-itemTypes	**Specifies type of items to recover, in this case Volume.**
-items	**Specifies a comma delimited list of volumes to be recovered.**
-backupTarget	**Specifies the volume containing the backup data to be recovered.**
-recoveryTarget	**Specifies the volume drive letter of the alternate volume to restore to.**

Example
To restore volume D, from backup version March 31, 2011, 9:00 to volume F (restored data are stored in volume E).

```
>Wbadmin start recovery –VersionIdentifiers:03/31/2011-09:00
–itemType:Volume –items:D: -backupTarget:E: -recoveryTarget:F:
```

11.5.4 Recover with the Windows Recovery Environment

Refer to the following instruction to perform a complete PC Restore with Windows Recovery Environment:

1. Insert the Windows Setup Disc into the CD / DVD drive.

2. Restart the computer.

   Note:
   In some cases, the computer manufacturer may have installed the Windows Recovery Environment directly to a partition on the hard drive.

   To access this partition, slowly tap the [F8] key after the BIOS information clears from the screen before the Windows startup menu.

3. Specify the language setting, and then click [Next].

Install Windows
Windows Vista
Language to install: English
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
Copyright © 2006 Microsoft Corporation. All rights reserved.
Next

4. Click [Repair your computer].

5. Setup will search the hard disk for existing Windows installation, then displays the result in [System Recovery Options].

6. Click [Next] afterward.

7. On the [System Recovery Options] page, click [System Image Recovery].

8. Perform one of the following actions:

   - Click [Use the latest available system image (recommended)] and then click [Next].

   - Click [Select a system image] and then click [Next].

9. If the [Select a system image] option is selected, perform one of the following actions on the [Select the location of the backup] page:

   - On the [Select the date and time of system image to restore] page, select the version to be restored, and then click [Next].

   - Click [Advanced] to browse for a backup on the network, and then click [Next].

10. On the [Choose how to restore the backup] page, perform the following optional tasks, and then click [Next]:

    - Select the [Format and repartition disks] check box to delete existing partitions and reformat the destination disks to be the same as the backup.

- Click the [Exclude disks button and then the checkbox beside the disk to be excluded from being formatted and partitioned.
- Select the [Only restore system disk] check box to perform an operating system only recovery.
- Click [Install drivers] to install drivers for the hardware to be recovering to.
- Click [Advanced] to specify whether the computer is restarted and the disks are checked for errors immediately after the recovery.

11. Confirm the details for the restoration, and then click [Finish] to begin the restore process.

12 Backup / Restore Windows System (ShadowProtect)

This chapter describes in details how to backup and restore Windows System with OBM (ShadowProtect System backup Module).

12.1 Supported versions

The ShadowProtect System backup module is supported for the following Windows platforms:

- Windows XP
- Windows Server 2003 / R2
- Windows Vista
- Windows 7
- Windows Server 2008 / R2
- Windows Small Business Server 2011

Note:
OBM does not support installation on Windows 2000.

12.2 Requirements and recommendations

Please ensure that the following requirements or recommendations are met by the backup client computer:

1. OBM and ShadowProtect are installed on the computer to be backed up.

2. Sufficient disk spaces are required for the temporary storage directory of the System backup.

   It is recommended to have free disk space of 150% x Total In-use Size of all volumes selected for backup.

   Note:
   The temporary storage directory cannot be set to a folder within a volume selected for backup.

12.3 Overview

The following steps are performed during a backup job:

1. Connection from the backup client to the backup server is established.

2. Download the server file list from the backup server.

3. Commands are issued to ShadowProtect to create the System backup data.

   For each volume selected for backup, a ShadowProtect backup image file (*.SPI* or *.SPF*) will be spooled to the temporary directory specified.

   - *.SPF*: A ShadowProtect full or base image file.
   - *.SPI*: A ShadowProtect incremental or differential image file.

4. Server and local file lists are compared to determine which file will be uploaded.

5. Delta file is generated (if necessary).

6. Data is encrypted, and uploaded to the backup server.

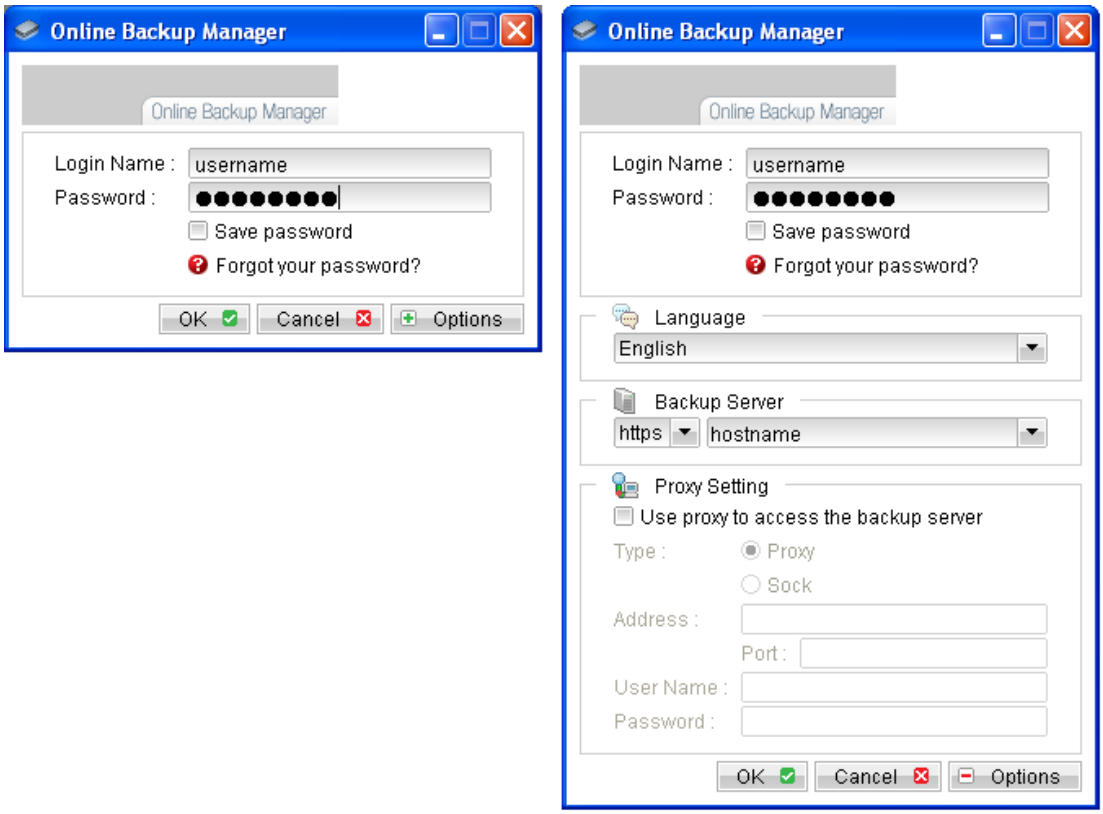
7. System backup data is removed from the temporary storage volume specified in the backup set.

8. Backup completed successfully.

12.4 How to backup Microsoft Windows System (ShadowProtect)

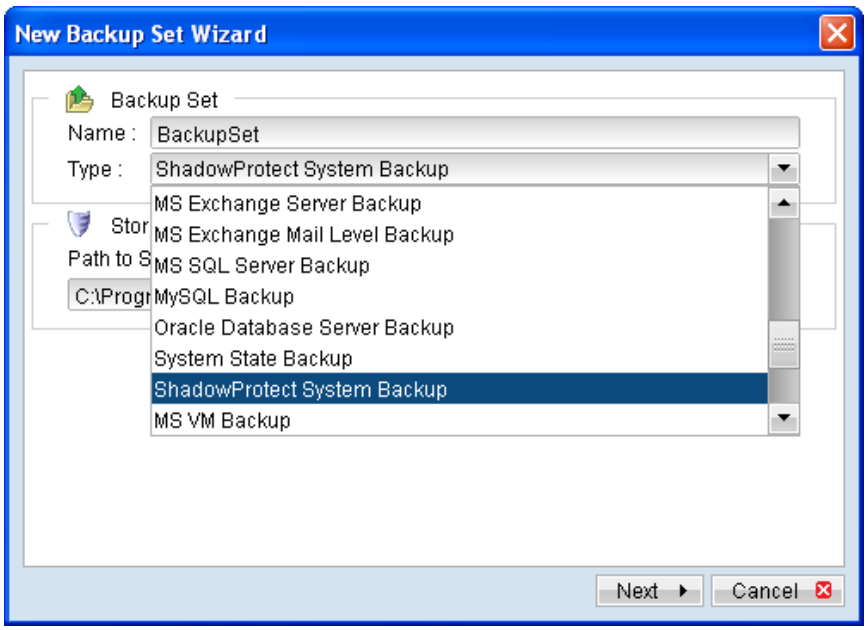
Refer to the following instructions to backup Windows System:

1. Login to the backup application's user interface.

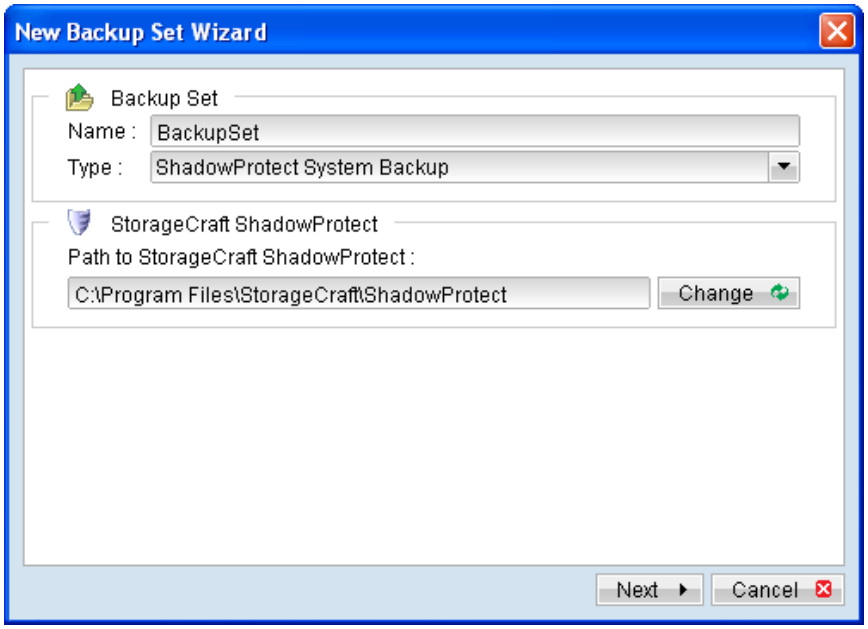


2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

3. Create a ShadowProtect System Backup set by selecting [ShadowProtect System Backup] from the backup set type dropdown menu.



4. Enter the path to the ShadowProtect installation.

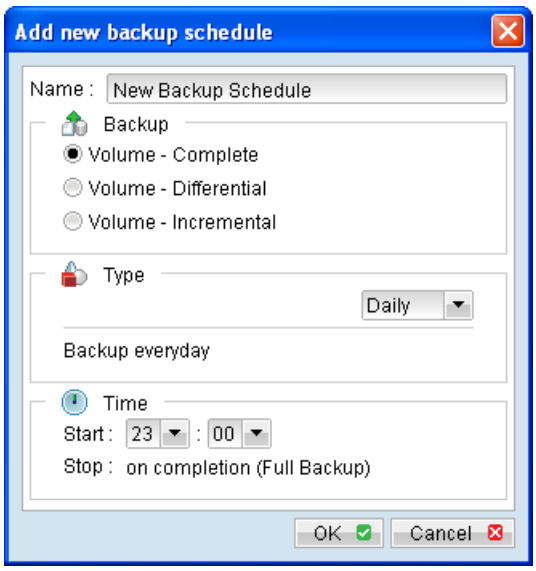


5. Select [Next] to proceed.

6. Select the corresponding volumes for backup.

7. Configure a backup schedule for unattended backups.

   Multiple backup schedules of different types can be configured for the same backup set.



Menu Items	Description
Volume - Complete	To perform a ShadowProtect Complete Backup - Base Image File (*.SPF)* contains the contents of a backup activity; it allows users to restore the contents of a computer system to a specific point-in-time.
Volume - Differential	To perform a ShadowProtect Differential Backup - Differential Image File *(.SPI*) contains the hard drive sectors that have changed since the Base Image File was created. Differential backup take about the same time to create as complete backup, but they are smaller. When restoring a drive, user must use the Base Image File with the appropriate Differential Image File to restore the computer to a specific point-in-time.
Volume - Incremental	To perform a ShadowProtect Incremental Backup - Incremental Image File *(.SPI*) contains the sectors that have changed since the last Incremental backup was taken. Incremental images are fast to create and smaller than either Full image files or

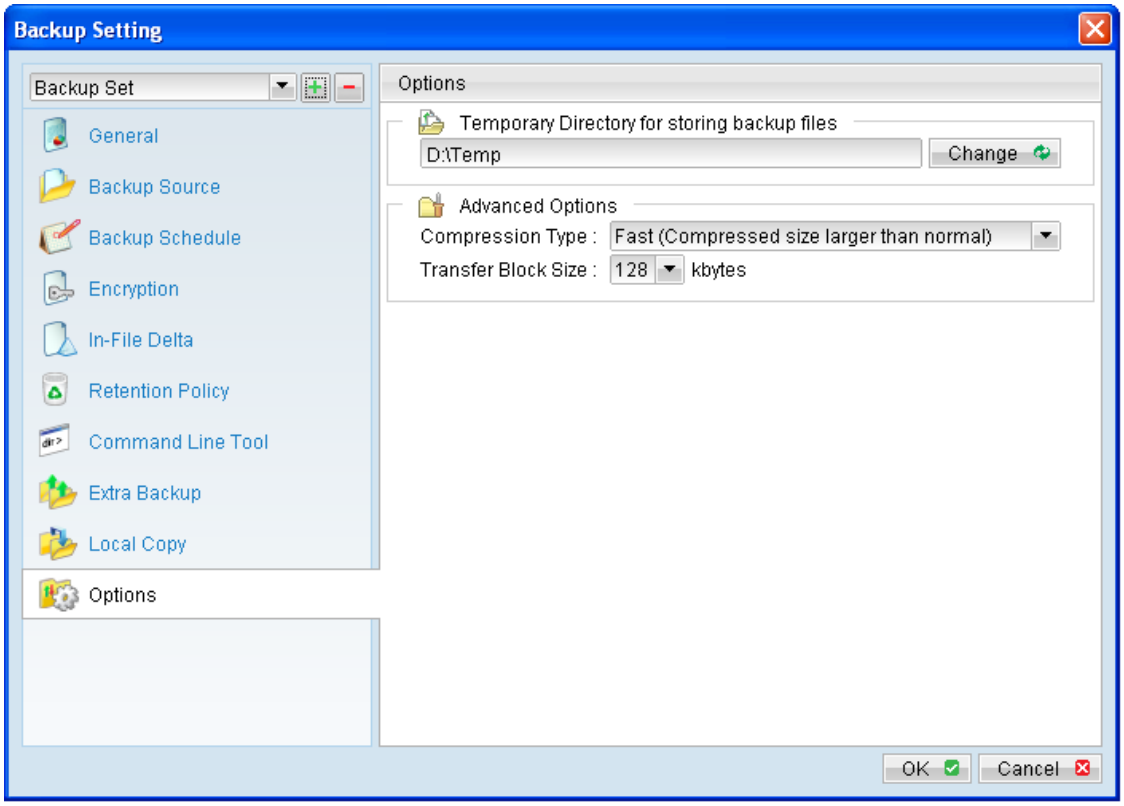
	Differential image files. When restoring a drive, you must use the Full image file and the appropriate Incremental image files necessary to restore the computer to a specific point-in-time.

8. Select an encryption setting for your backup set.

9. Press the [OK] button to complete the configuration of backup set.

10. Configure the temporary directory of the backup set.

11. On the OBM main menu, press [Backup Setting], then [Options].



12. Click [Change] and select the temporary directory for backup.

    Note:
    The temporary storage directory cannot be set to a folder within a volume selected for backup.

    Also, please ensure sufficient disk space is allocated for the backup operation.

13. Scheduled backup will run automatically at the configured schedule time.

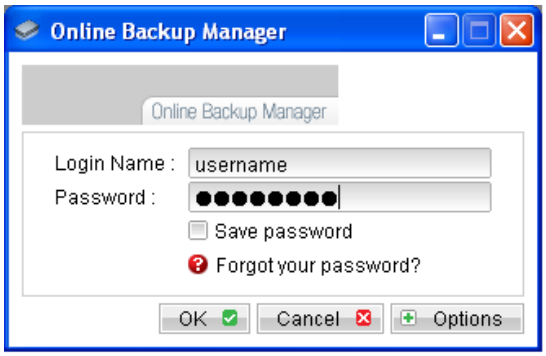
14. Click [Backup] button on the left panel to perform a backup immediately.

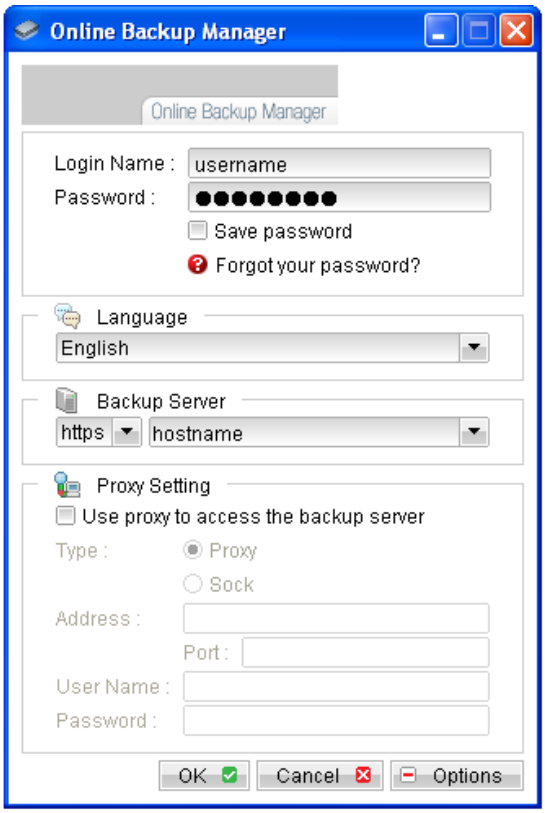
12.5 How to restore Microsoft Windows System (ShadowProtect)

Refer to the following instructions to restore a Windows System:

1. Install OBM on the machine to be restored to.

2. Login to the backup application's user interface.





3. Select the [Restore] button and the corresponding backup set.

4. Select the System file to be restored and its restore destination.

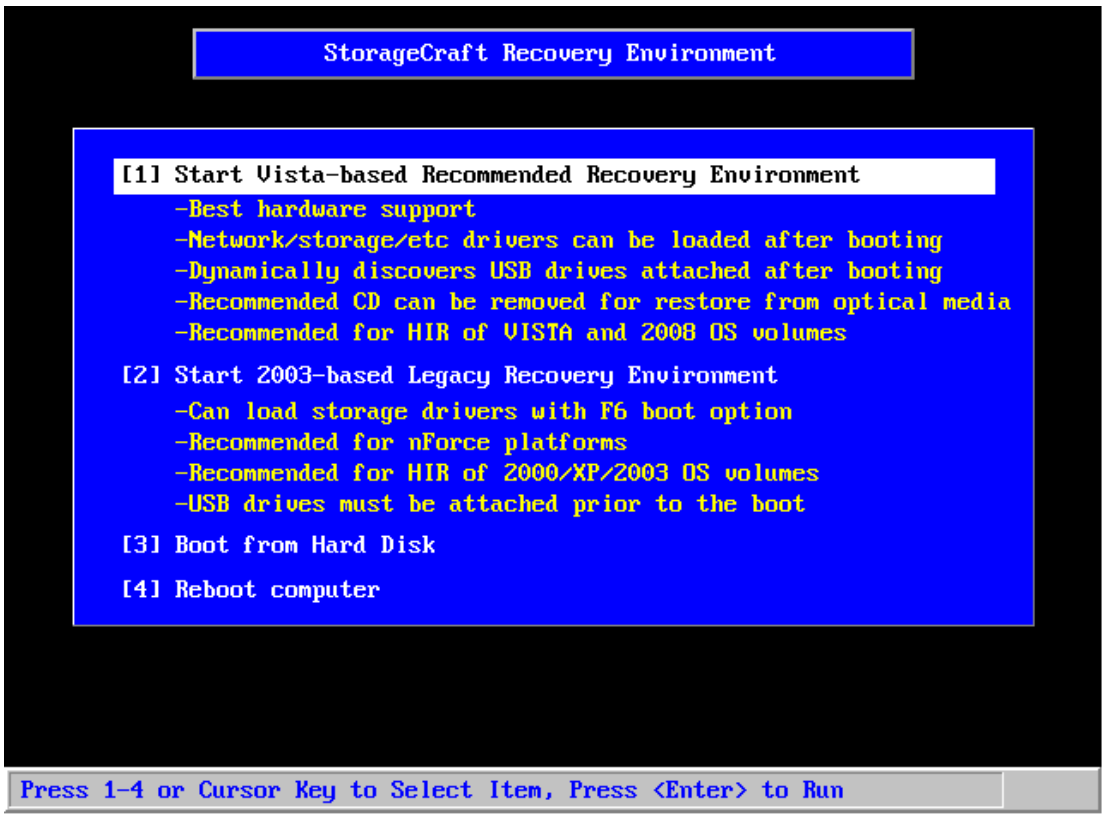
5. Click the [Start Restore] button to begin the restore process.

6. To restore a system volume (operating system volume), you need to start the computer in StorageCraft Recovery Environment.

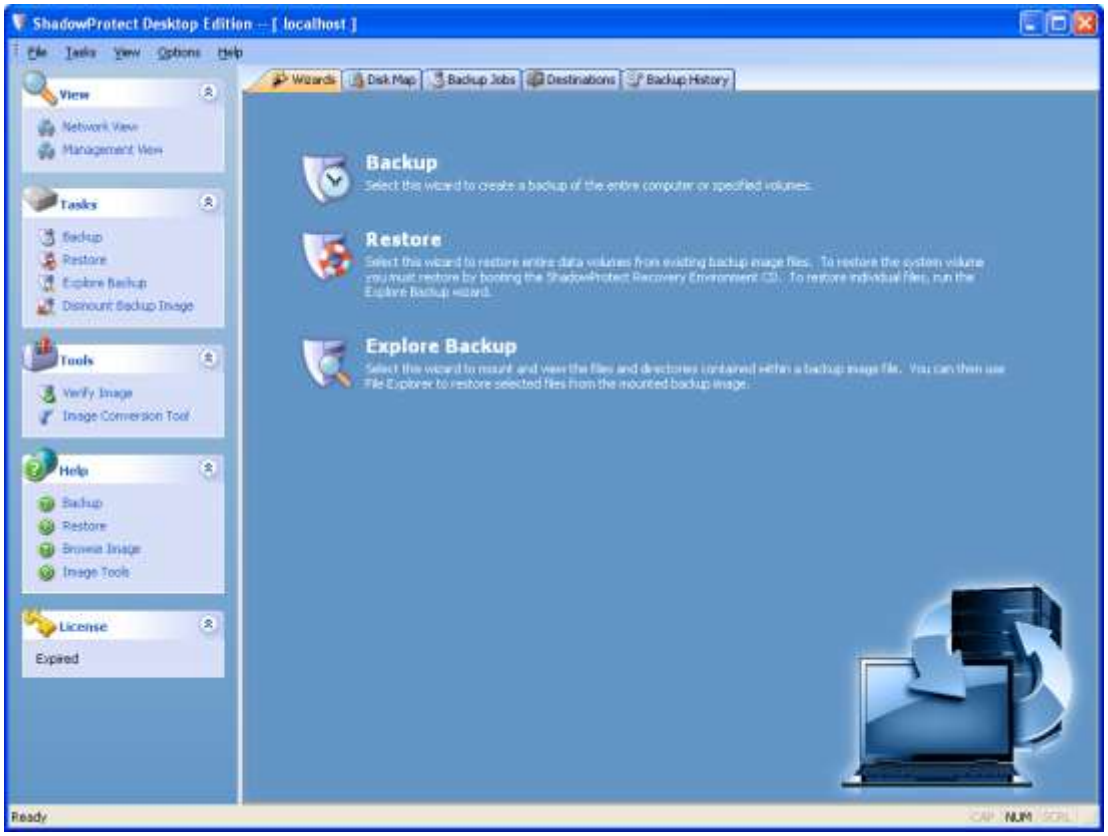
   - Insert the ShadowProtect Disc into the CD / DVD drive.
   - Restart the computer.

   Note:
   In some case, you may need to press the required key to boot up from disc.

   - Select the corresponding option according to the OS platform.


StorageCraft Recovery Environment
[1] Start Vista-based Recommended Recovery Environment
-Best hardware support
-Network/storage/etc drivers can be loaded after booting
-Dynamically discovers USB drives attached after booting
-Recommended CD can be removed for restore from optical media
-Recommended for HIR of VISTA and 2008 OS volumes
[2] Start 2003-based Legacy Recovery Environment
-Can load storage drivers with F6 boot option
-Recommended for nForce platforms
-Recommended for HIR of 2000/XP/2003 OS volumes
-USB drives must be attached prior to the boot
[3] Boot from Hard Disk
[4] Reboot computer
Press 1-4 or Cursor Key to Select Item, Press <Enter> to Run

7. To restore a non system volume (non operating system volume), in Windows, start the ShadowProtect user interface.



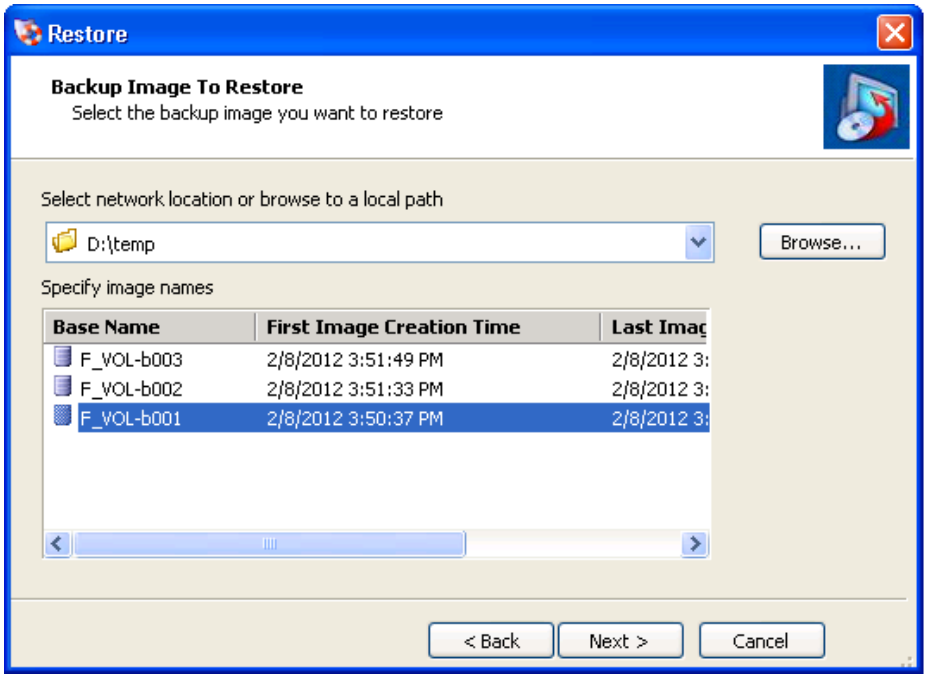
8. Click [Restore] to start the Restore Wizard.

9. Press [Next] to proceed.

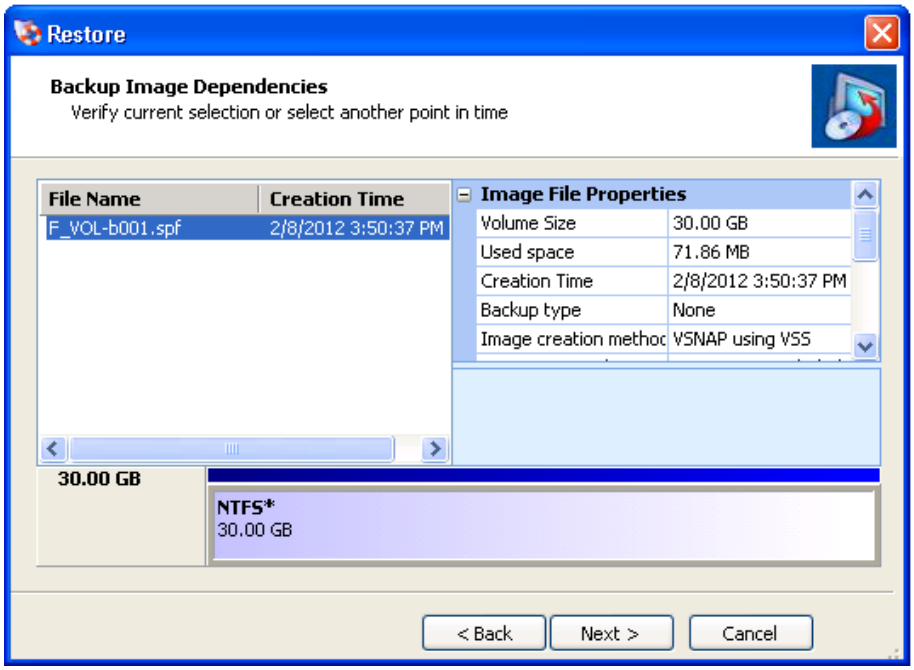
Restore
Welcome to the Restore Wizard!
This wizard will help you to restore entire data volumes from existing backup image files. To restore the system volume you must restore by booting the ShadowProtect Recovery Environment CD. To restore individual files, run the Explore Backup wizard.
Press Next to continue
< Back
Next >
Cancel

10. Browse to the image file restored from the OBS server. The destination locations can be a local directory or network share.

    Click [Next] to continue.



11. In the Backup Image Dependencies dialog screen, any ShadowProtect Differential or Incremental image associated with the Full image will be displayed.



Select an image file to view its properties, including:

- Image File Properties -
  Volume size, creation time, compression, password protection, and comment.

- Original Partition Information -
  Style, number, type, bootable option, starting offset and length.

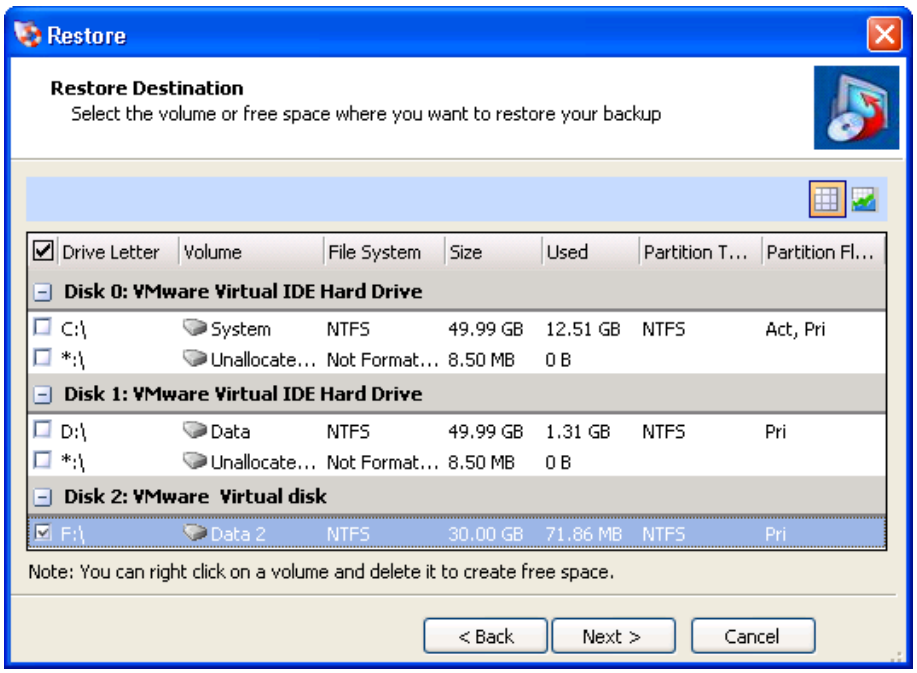
- Disk Information –
  Disk geometry, disk size and number of the first track sectors.

  A user also views the disk layout graphically at the bottom of the screen.

- Originating machine –
  The operating system version, the machine name, MAC address and the engine version of ShadowProtect used to create the image file.

Click the [Next] to continue.

12. In the Restore Destination dialog screen, select the destination volume for the image to be restored to.


Restore
Restore Destination
Select the volume or free space where you want to restore your backup
Drive Letter
Volume
File System
Size
Used
Partition T...
Partition Fl...
Disk 0: VMware Virtual IDE Hard Drive
C:\ System NTFS 49.99 GB 12.51 GB NTFS Act, Pri
*:\ Unallocate... Not Format... 8.50 MB 0 B
Disk 1: VMware Virtual IDE Hard Drive
D:\ Data NTFS 49.99 GB 1.31 GB NTFS Pri
*:\ Unallocate... Not Format... 8.50 MB 0 B
Disk 2: VMware Virtual disk
F:\ Data 2 NTFS 30.00 GB 71.86 MB NTFS Pri
Note: You can right click on a volume and delete it to create free space.
< Back
Next >
Cancel

The following options are available by right clicking on the volumes:

- Delete Volume -
  This will delete a volume. The deleted volume will become unassigned space on the disk that can be repartition.

- Set Active –
  This will set the volume active.

  Only one partition may be designated as active. By setting a volume active, the computer will boot to the volume.

- Create an exact primary partition –
  Allows user to define and create a primary partition on the disk.

  The maximum number of primary partitions on the same disk is 4.

- Create extended partition –
  Allows user to extend a partition and then subdivide this partition in to one or more logical partitions.

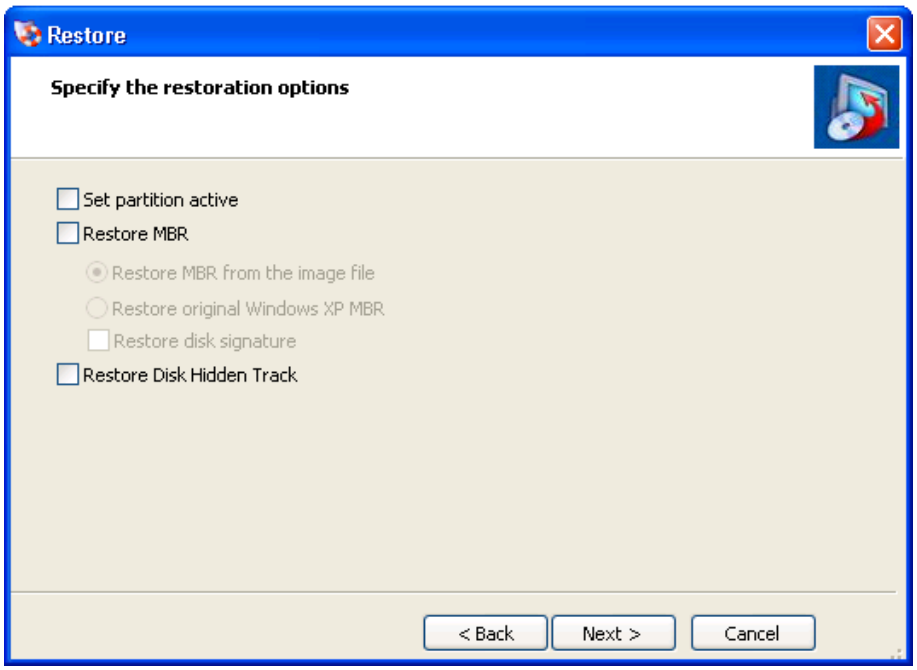
Note:
Restoring a backup image to a volume overwrites all data currently on the volume.

Furthermore, there must be sufficient disk space to restore the backup image. For example, a user cannot restore a 4GB backup file with only 1GB of free space.

Click [Next] to continue.

13. In the Specify the restoration options dialog screen, please review all of the options available.

    All of these options are important where restoring an operating system volume on a computer.



- Set Partition Active -
  This will make the restored drive the active partition (the drive that the machine boots from).

- Restore MBR –
  Restore the master boot record.

  The master boot record is contained in the first sector of the first physical hard drive; it consists of a master boot program and a partition table that describes the disk partitions.

  The master boot program looks at the partition table to see which primary partition is active. It then starts the boot program from the boot sector of the active partition.

  You can restore the MBR from the image file that was saved with the backup image or you can restore an original Windows MBR.

- Restore disk signature –
  Restores the original physical disk signature of the hard drive.

  Disk signatures are included in Windows Server 2003, and are necessary before the hard drive can be used.

- Restore Disk Hidden Track –

Restore the first 63 sectors of a drive, some boot loaded applications required this for the system to boot.

Click [Next] to continue.

14. Review the Restore Wizard Summary; click [Finish] to begin the restore process.

    Restore process can be viewed by clicking on the [Volume Restore] tab associated with the restore job.

13 Backup / Restore VMware Virtual Machines

This chapter describes how to backup and restore virtual machine running on VMware.

13.1 Backup virtual machines running on VMware ESXi / ESX Server

13.1.1 Supported versions

The VMware VM backup module is supported for the following VMware ESXi / ESX versions:

- VMware ESXi 3.5
- VMware ESXi 4.0
- VMware ESXi 4.1
- VMware ESXi 5.0

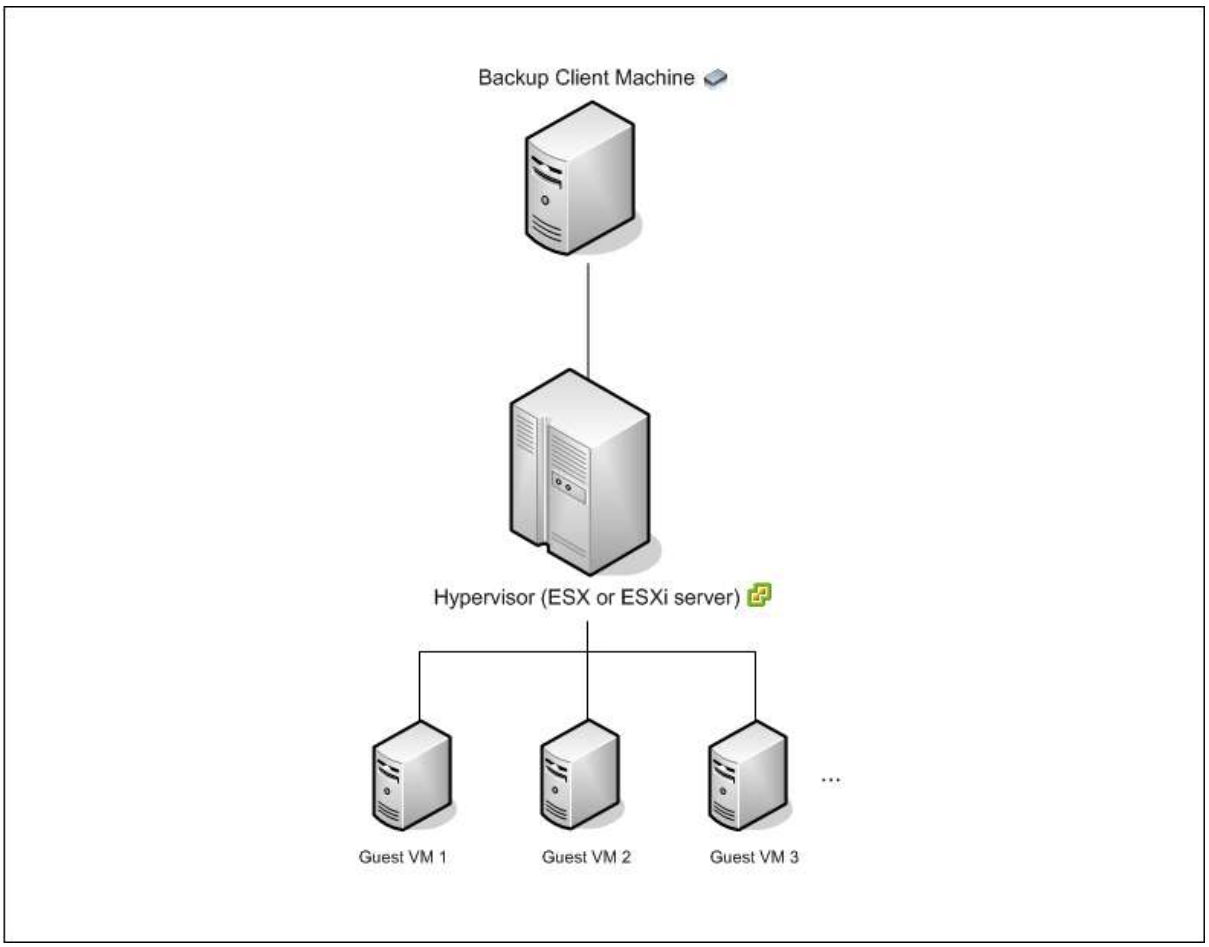
- VMware ESX 3.5
- VMware ESX 4.0
- VMware ESX 4.1

For more details, please refer to Help Centre Article:
https://help..com/openArticle.aspx?aid=2323

13.1.2 Requirements and recommendations

OBM cannot be installed on the hypervisor (ESX or ESXi server).

A separate dedicated physical machine – the Backup Client Computer - must be used for backup of your virtual machines.



Please ensure that the following requirements or recommendations are met by the Backup Client Computer:

1. The Backup Client Computer is running on a supported OS platform:

   - Windows
   - Mac OS X
   - Linux

2. OBM version 6.7 or above is installed on the backup client computer.

3. The following TCP ports must be opened on the Backup Client Computer:

   - Port 22
   - Port 80 and 443

4. For better performance, OBM is recommended to be installed on a 64 bit computer, with multiple CPUs and cores.

5. For Backup Client Computer running on Linux, GUI environment must be installed (e.g. GOME or KDE).

6. Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation.

7. It is recommended that the temporary directory have disk space of at least 50% of the largest sized virtual machine to be backed up.

8. It is recommended that the temporary directory be configured on a local drive.

9. It is recommended that the temporary directory is not configured on the same partition which the operating system is installed on.

10. For backup of virtual machine with snapshot, backup of the whole VM instead of individual disk is highly recommended.

11. Consider performing routine recovery test to ensure your backup is setup and performed properly.

Please ensure that the following requirements are met by the Hypervisor:

1. SSH must be enabled on the Hypervisor.

2. The root account must be enabled.

   OBM ESX / ESXi backup set requires the root account for backup and restore.

3. The following TCP ports must be opened on the hypervisor:

   - Port 22
   - Port 80 and 443

4. It is recommended that the datastore have disk space of the largest sized virtual machine to be backed up.

13.1.3 Limitations

The following are limitations of the VMware VM backup module:

1. VMware ESX or ESXi Server with Raw Device Mapping (RDM) is not supported.

   Snapshots are not available when the Raw Device Mapping (RDM) is used in physical compatibility mode.

2. VMware ESX Server Cluster (Resource Pool) is not supported.

3. Backup of virtual machine with multiple snapshot root branches is not supported on VMware ESXi Server version 4.0 and 4.1.

4. For backup of individual virtual disk, the restored virtual machine does not support the reversion of previous snapshots, if the snapshot contains disks which are not previously backed up by OBM.

5. For virtual machines with Independent Disks:

   - If Independent Disks are to be included in the virtual machine backup, the virtual machine must be powered off first, before running the backup job.

   - If the virtual machine is powered on, the Independent Disk will not be backed up.

     OBM will skip the snapshot creation of any Independent Disk on the virtual machine.

13.1.4 Overview

The following steps are performed during a backup job:

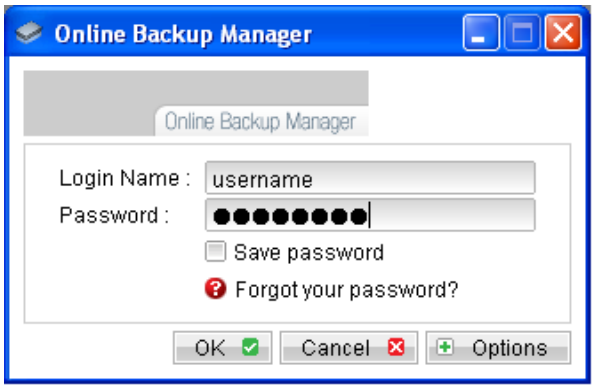
1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Connection from the backup client to the hypervisor is established.
4. Commands are issued to the hypervisor to create snapshot of the virtual machine for backup
5. Server and local file lists are compared to determine which file will be uploaded.
6. Delta file is generated for modified file (if necessary).
7. Existing, and snapshot data are encrypted, compressed, and streamed to the backup server.
8. Commands are issued to the hypervisor to remove snapshot created for backup.
9. Backup completed successfully.

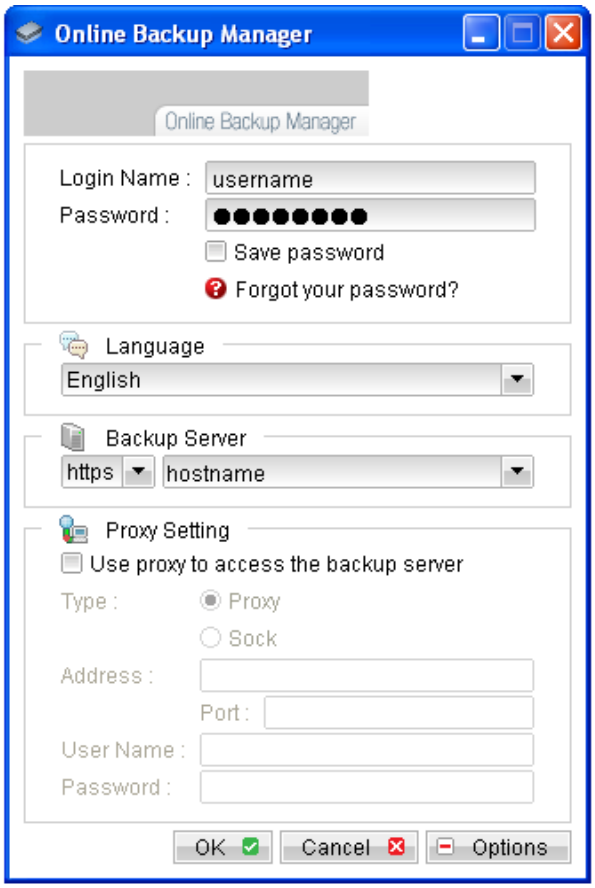
13.1.5 How to backup virtual machines on VMware ESXi / ESX Server

Refer to the following instructions to backup VM running on VMware ESXi or ESX Server:

1. Login to the backup application's user interface.

   For backup client computer on Windows, double-click on the OBM desktop icon or right-click on the system tray icon:



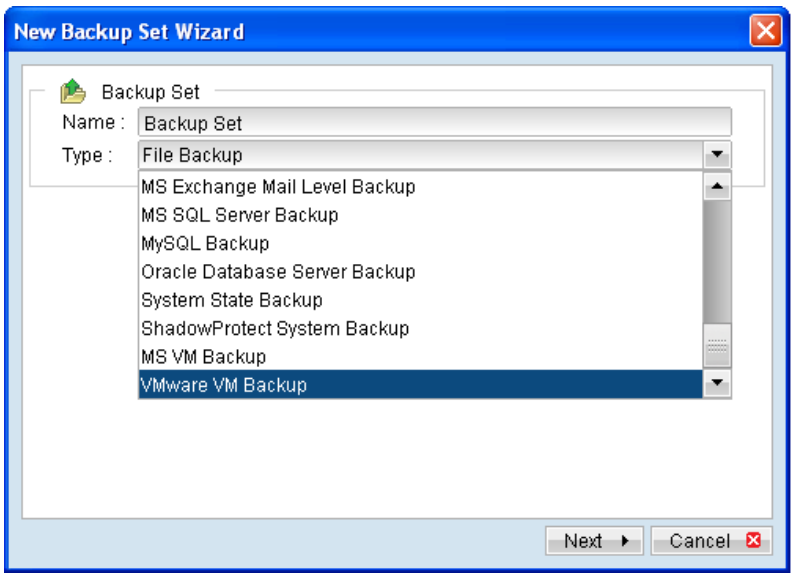


For backup client computer on Mac OS X, double-click on the OBM desktop icon.

For VMware Server installation on Linux, enter the following command to start the OBM graphical user interface:

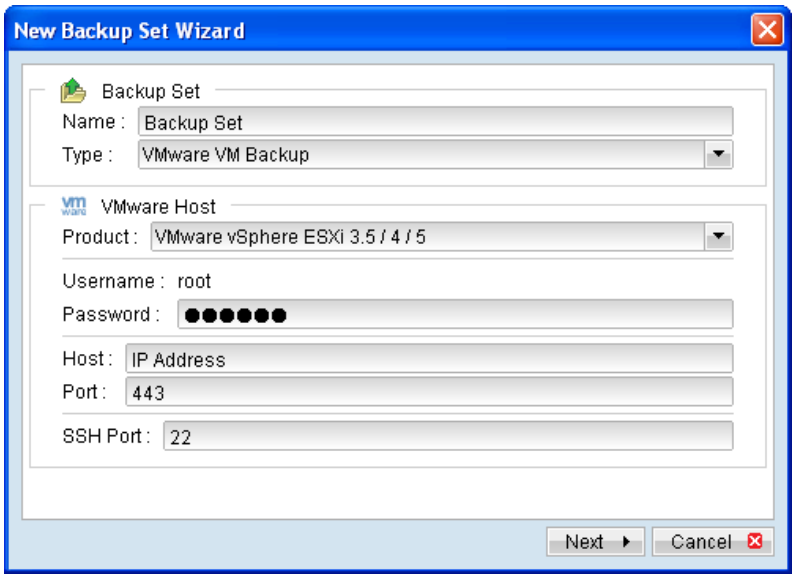
```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.



3. Create a VMware VM Backup set by selecting [VMware VM Backup] from the backup set type dropdown menu.

4. Enter the corresponding information required:

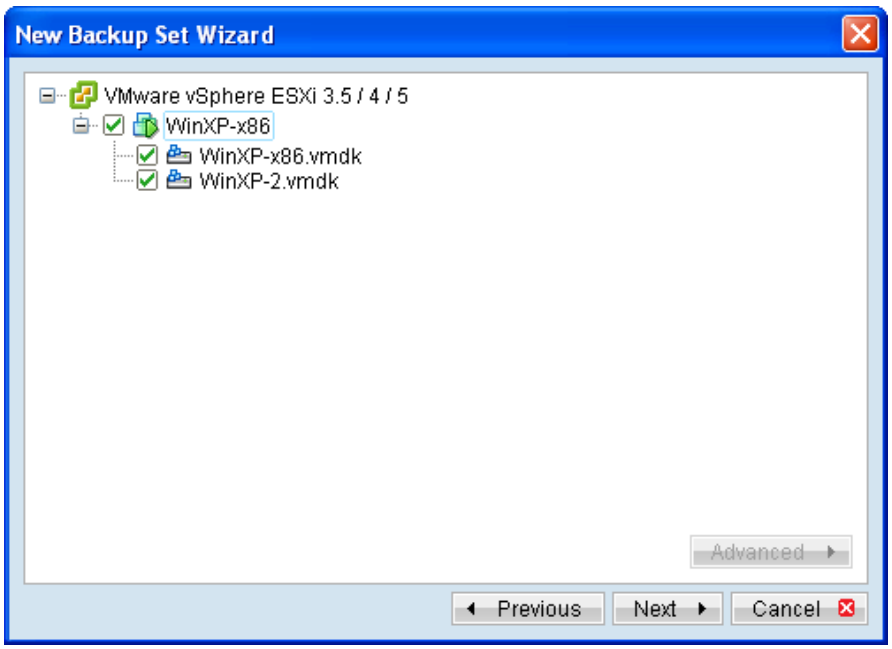


Menu Items	Description
Name	Enter a backup set name of your choice.
Type	Select backup set type [VMware VM Backup].
VMware Host Version	Select version [VMware vSphere ESXi] or [VMware vSphere ESX] according to your setup.
Username	The username must be root
Password	Enter the password for the root account.

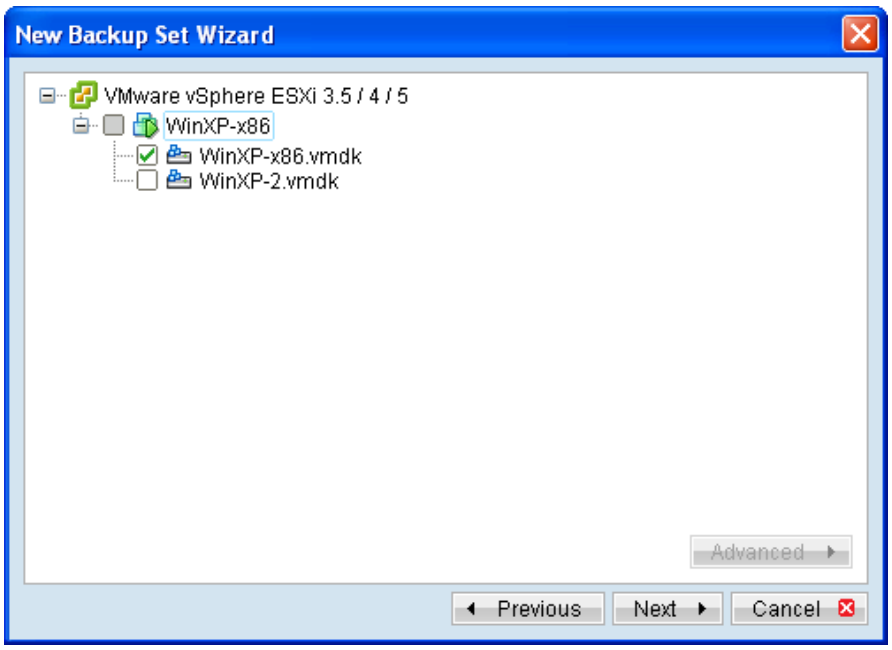
Host	Enter the IP address or hostname of your hypervisor.
Port	Enter 80 for connection via HTTP protocol or 443 for HTTPS protocol.
SSH Port	Enter the SSH port (default: port 22).

5. Select [Next] to proceed.

6. Select the corresponding virtual machines for backup.



7. Alternatively, select individual virtual disk for backup by expanding the corresponding VM sub tree.



Note:
For backup of individual virtual disk, configuration files of the VM are also backed up.

Important:
For backup of VM with snapshot, backup of the whole VM instead of individual disk is highly recommended.

8. Configure a backup schedule for unattended backups.

   Note:
   Multiple backup schedules of different types can be configured for the same backup set.

9. Select an encryption setting for your backup set.

10. Press the [OK] button to complete the configuration of backup set.

11. Scheduled backup will run automatically at the configured schedule time.

12. Click [Backup] button on the left panel to perform a backup immediately.

13.1.6 How to restore virtual machines on VMware ESXi / ESX Server

Refer to the following instructions to restore VM running on VMware ESXi or ESX Server.

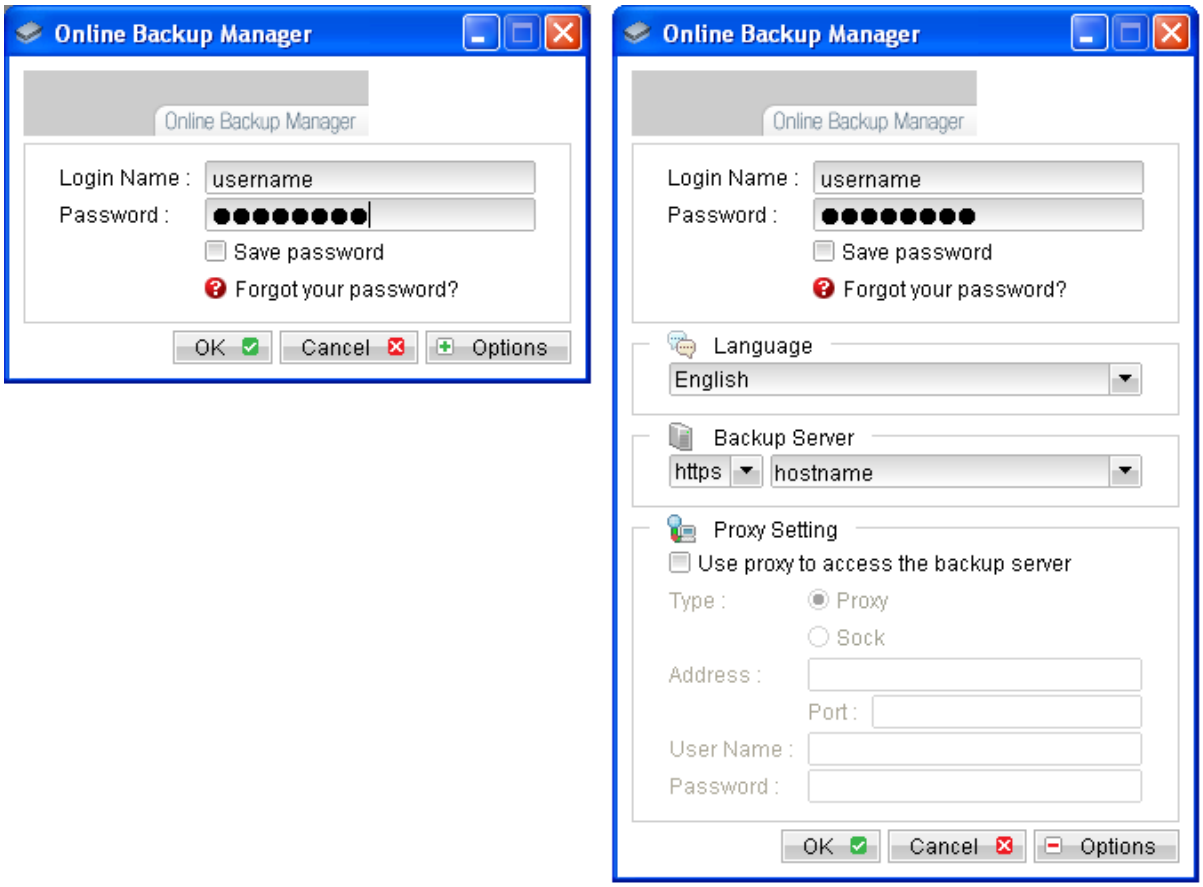
VM can be restored to the original location with the following condition:

- If the VM to be restored does not exist on the original hypervisor, the VM will be restored as a new virtual machine.
- If the VM to be restored still exist on the original hypervisor, the existing VM will be replaced by the backed up version.

13.1.1.6 How to restore virtual machines to the original hypervisor

1. Login to the backup application's user interface.

For backup client computer on Windows, double-click on the OBM desktop icon or right-click on the system tray icon:

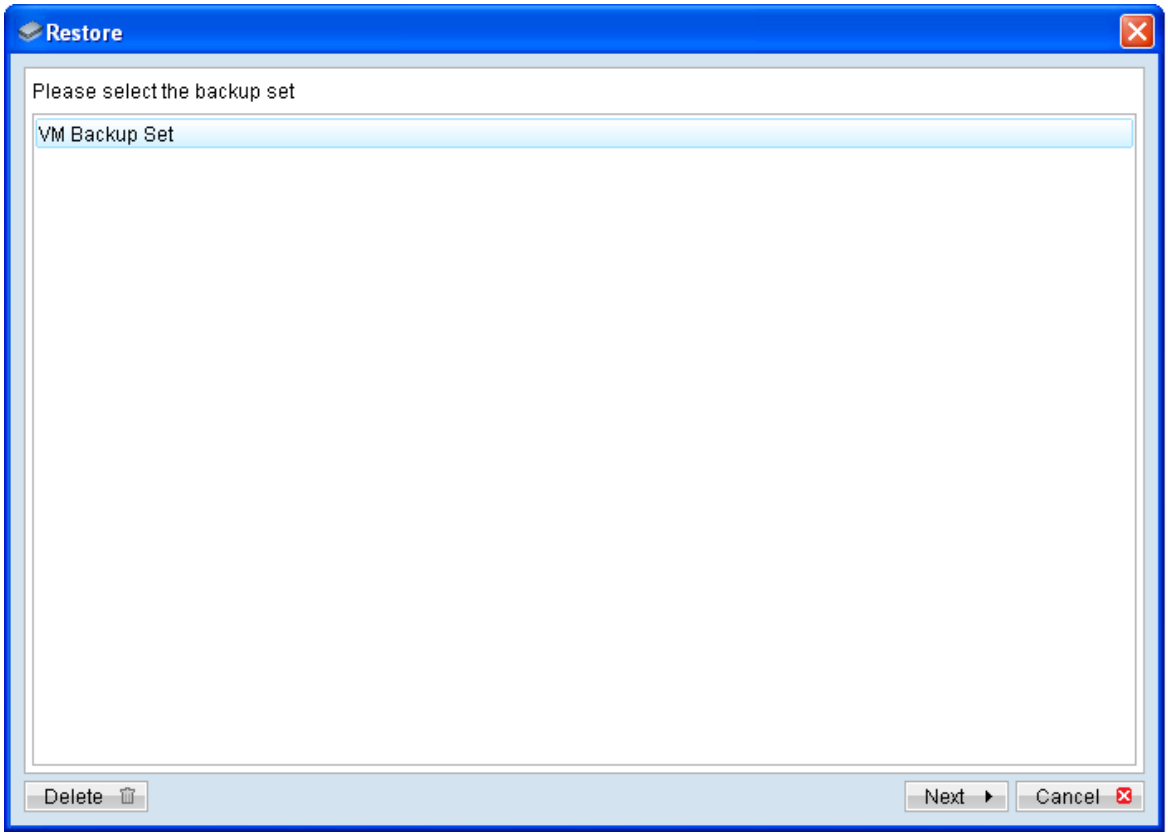


For backup client computer on Mac OS X, double-click on the OBM desktop icon.

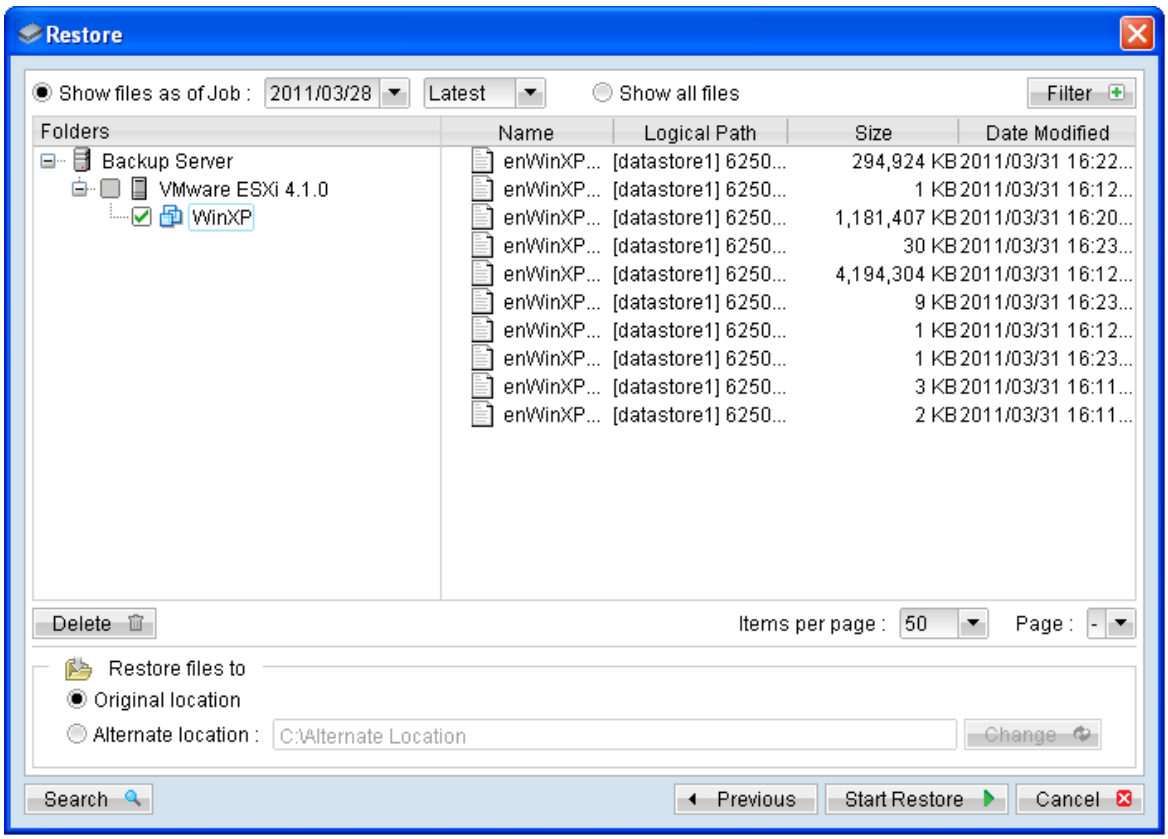
For VMware Server installation on Linux, enter the following command to start the OBM graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Restore] button and the corresponding backup set.

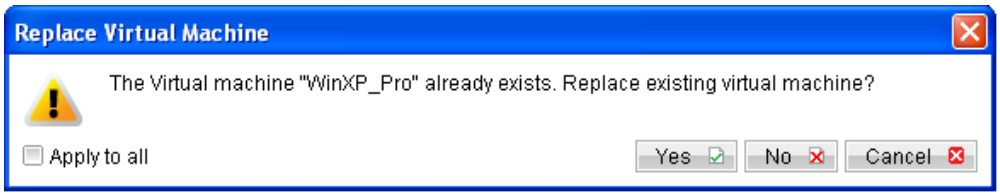


3. Select the virtual machines to be restored and choose [Original Location] for restore files to.



4. Click the [Start Restore] button to begin the restore process.

5. User will be prompted if a virtual machine selected to be restored exist on the hypervisor.



6. When the restore process is completed, the virtual machines will be restored to the original hypervisor.

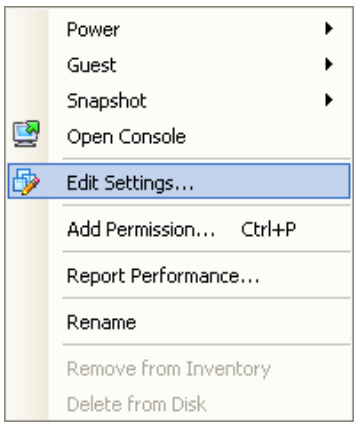
7. For any virtual disk that was not restored (e.g. original backup source did not include all hard disks configured for the VM).

   Continue to the next steps for instruction to remove the missing hard disk from the virtual machine's configuration.

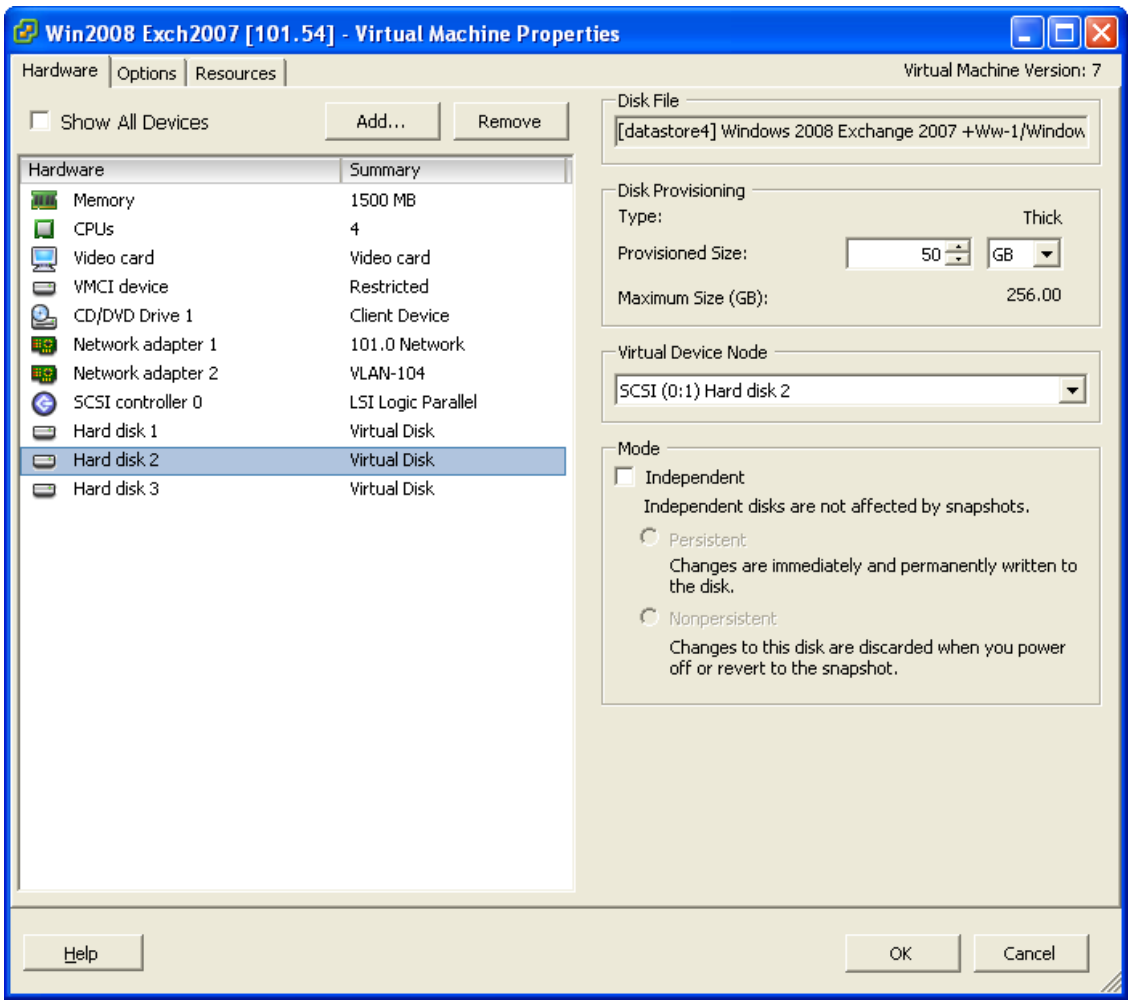
For original virtual machine with no snapshot

1. Open VMware vSphere Client.

2. Under inventory, right click on the newly restored virtual machine, select [Edit Settings].



3. For each virtual disk that was not restored, remove the corresponding [Hard disk] from [Hardware].

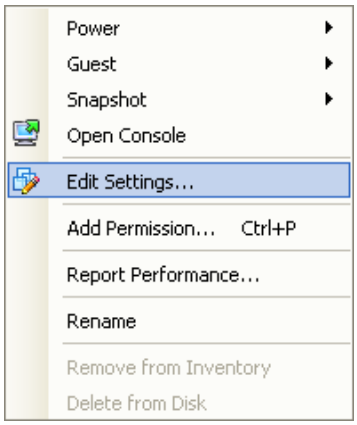


4. Start the virtual machine afterward.

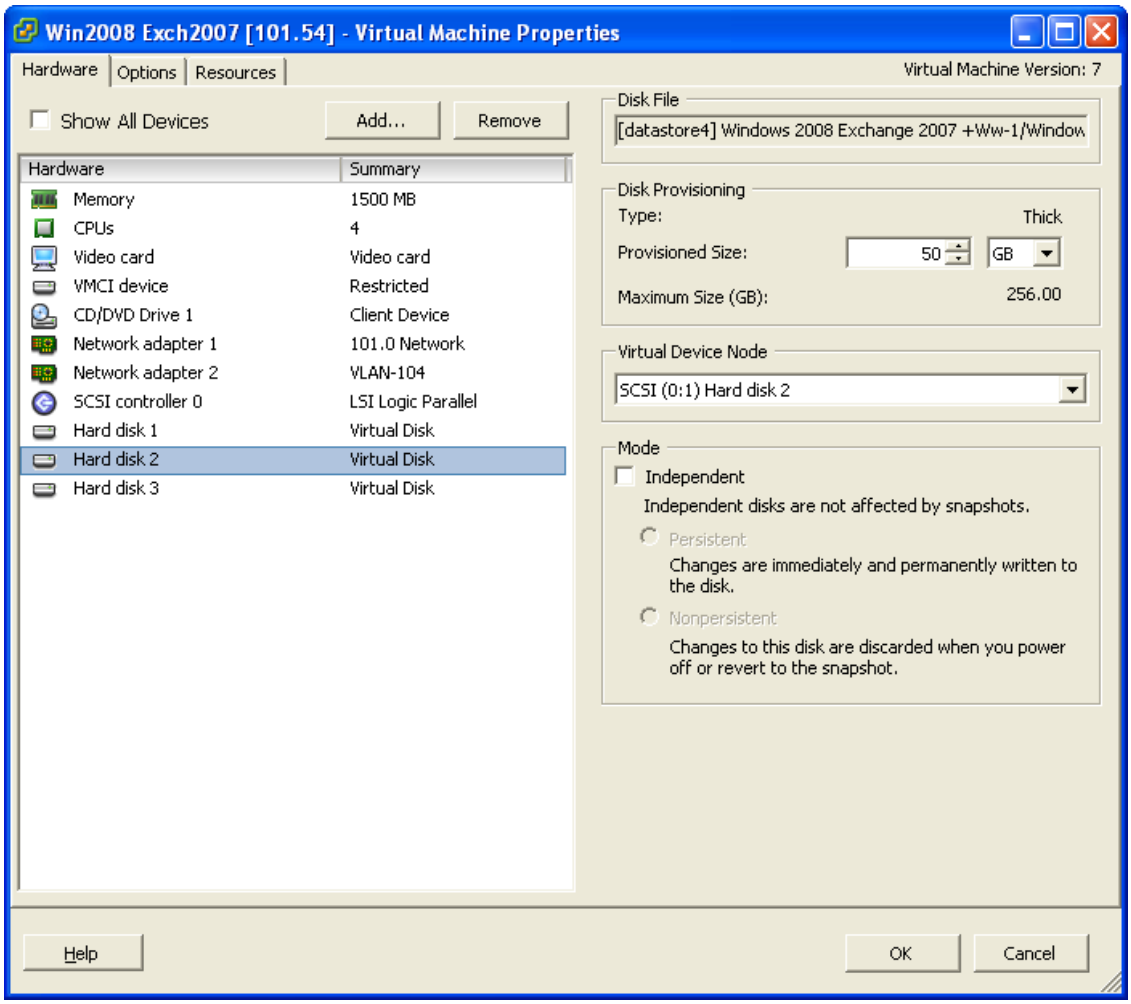
For original virtual machine with snapshot

1. Open VMware vSphere Client.

2. Under inventory, right click on the newly restored virtual machine, select [Edit Settings].

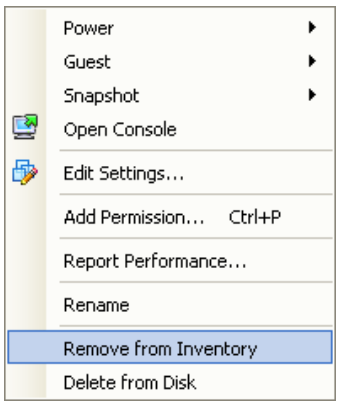


3. For each virtual disk that was not restored, remove the corresponding [Hard disk] from [Hardware].



4. Remove the VM from inventory.

5. Right click on the newly restored virtual machine; select [Remove from Inventory].



6. Locate the virtual machine's folder location on the hypervisor.

   Important:
   Serious problem may occur if the configuration files are incorrectly modified; it may prevent the virtual machine from starting.

   Please only perform the following procedures if you have in-depth knowledge on VMware product.

7. Delete the lines of the removed virtual disk.

   - Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

   ```
   ${VM-Location}\${VM-Name}.vmsd
   ```

   - Locate the line of all non existing virtual disk.

   Example:

   Snapshot 1, SCSI (0:2) Disk 2 is removed.

```
.encoding = "UTF-8"
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
snapshot0.disk2.fileName = "Windows 2008-2.vmdk"
```

```
snapshot0.disk2.node = "scsi0:2"
```

- Remove the corresponding lines.

```
.encoding = "UTF-8"
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Perform the same steps for each snapshot.
- Save the changes afterward.

8. Update the number of virtual disk.

- Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

```
${VM-Location}\${VM-Name}.vmsd
```

- Locate the *numDisks* parameter.

Example:

Snapshot 1, if one of the disks is removed, updates the value of *snapshot0.numDisks*

```
.encoding = "UTF-8"
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
```

```
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Modify the line from:

snapshot0.numDisks = "3"

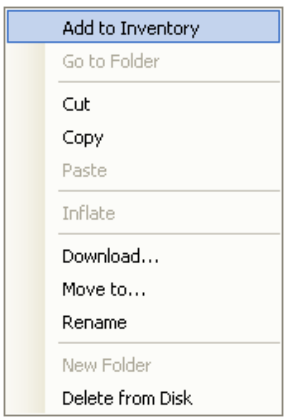
To

snapshot0.numDisks = "2"

```
.encoding = "UTF-8"
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "2"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Perform the same steps for each snapshot.
- Save the changes afterward.

9. Add the VM back into the inventory.



10. Remove any existing snapshot.

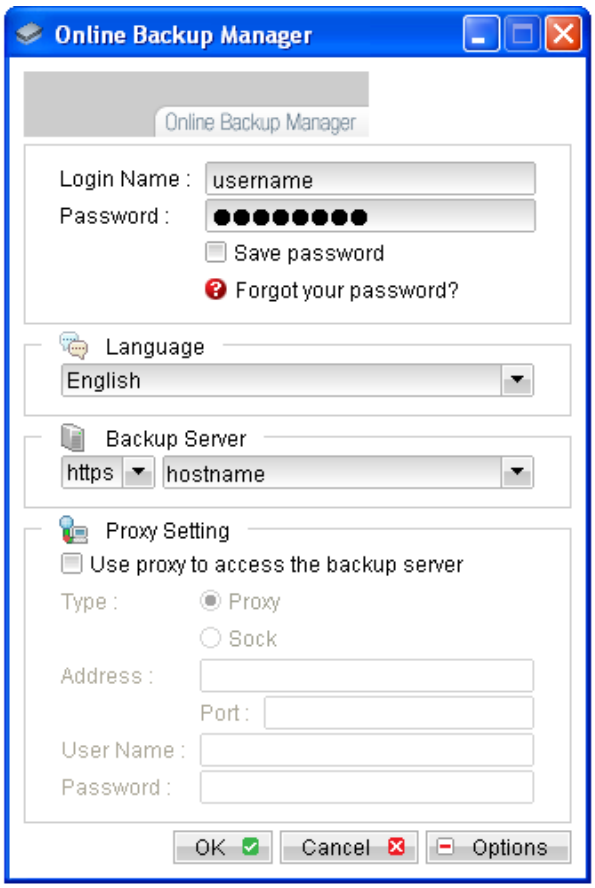
Important:
The restored virtual machine does not support the reversion of previous snapshots if they contain virtual disks not restored.

11. Start the virtual machine.

13.1.2.6 How to restore virtual machines to another hypervisor

1. Login to the backup application's user interface.

For backup client computer on Windows, double-click on the OBM desktop icon or right-click on the system tray icon:

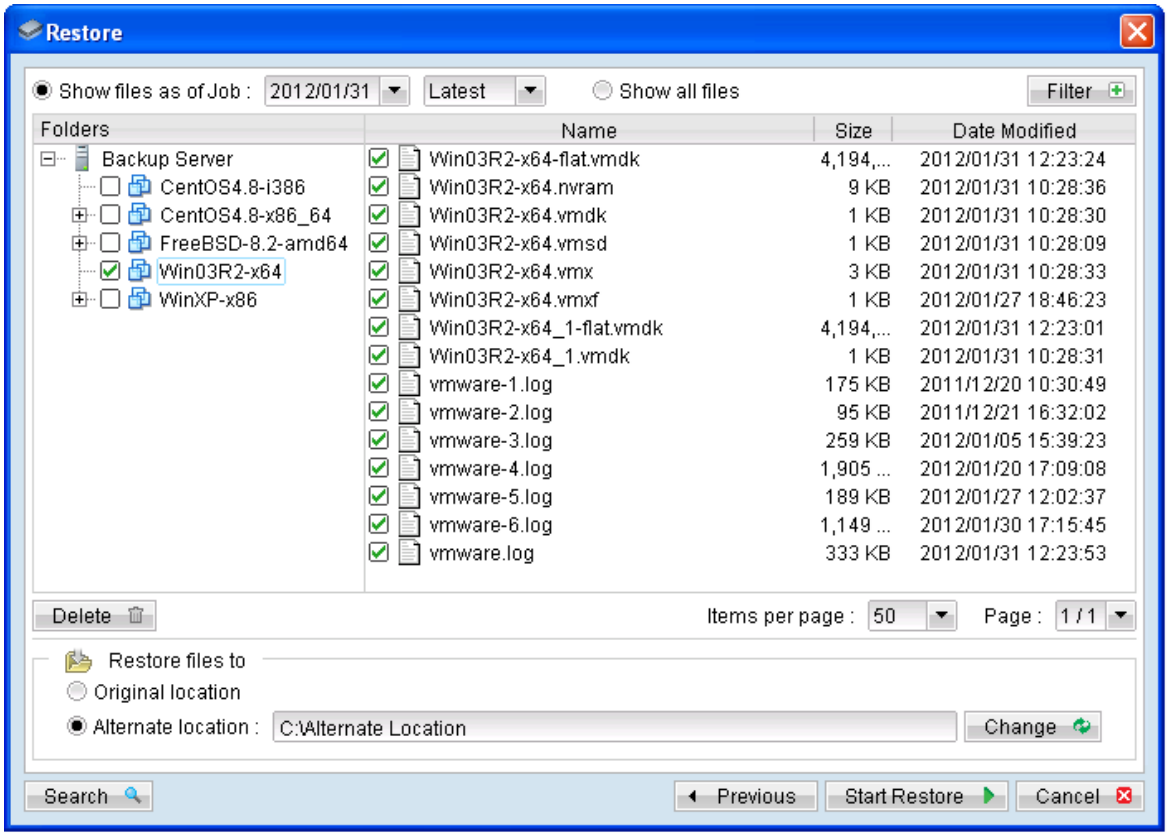


For backup client computer on Mac OS X, double-click on the OBM desktop icon.

For VMware Server installation on Linux, enter the following command to start the OBM graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Restore] button and the corresponding backup set.



3. Select the virtual machines to be restored and choose [Alternate location] for restore files to.

   Restore of individual virtual disk is only supported for restore to [Alternation location].

4. Click on the [Change] button and browse to the directory path which you would like to restore the data to.

5. Click the [Start Restore] button to begin the restore process.

6. When the restore process is completed, data of the selected virtual machines will be restored to the specific location.

7. Register the virtual machines on the new hypervisor.

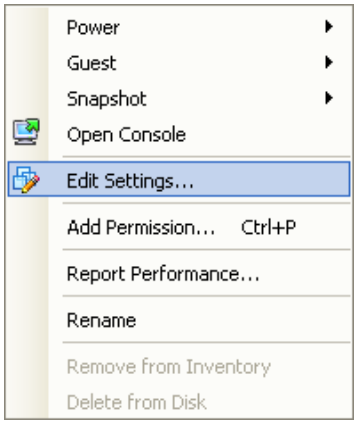
8. <u>For any virtual disk that was not restored</u> (e.g. original backup source did not include all hard disks configured for the VM).

   Continue to the next steps for instruction to remove the missing hard disk from the virtual machine's configuration

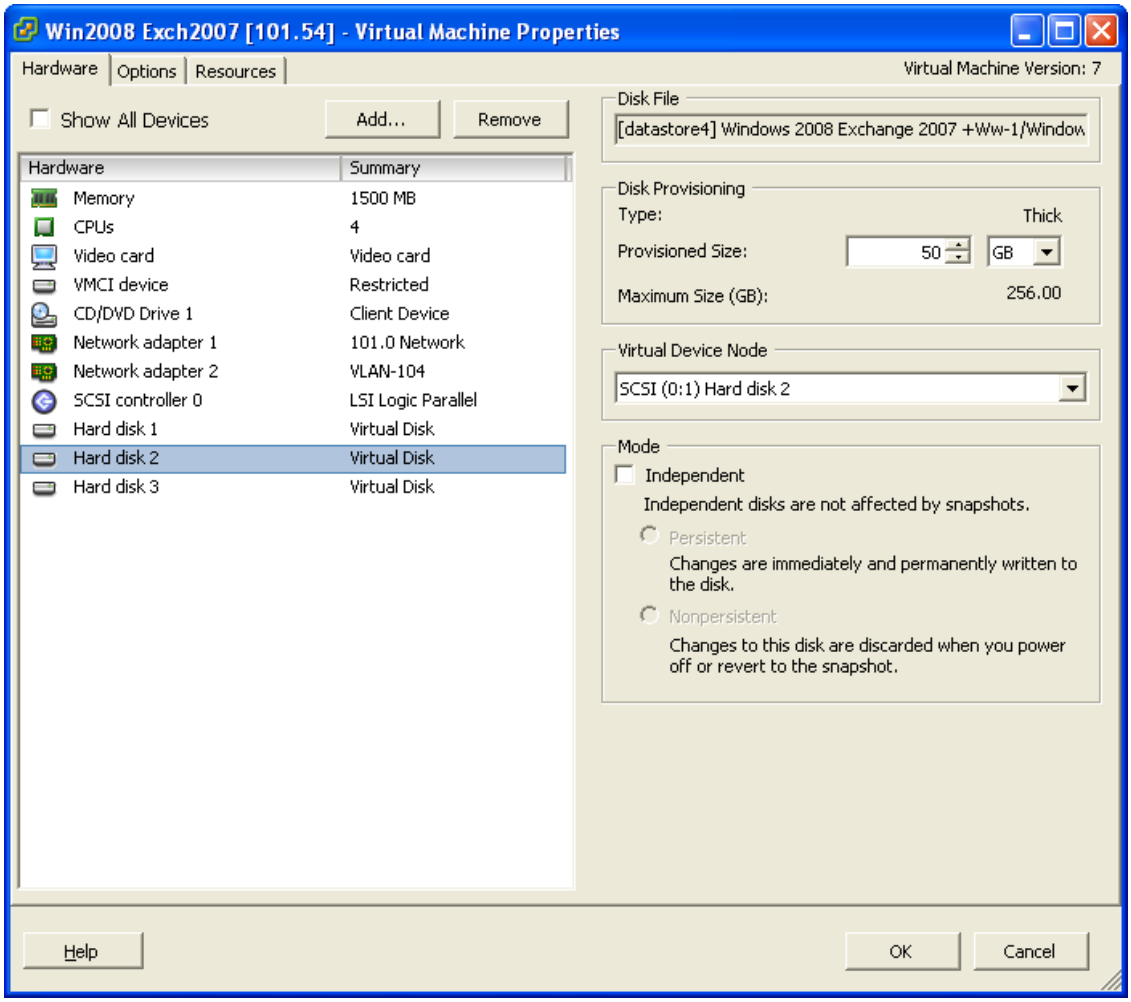
<u>For original virtual machine with no snapshot</u>

1. Open VMware vSphere Client.

2. Under inventory, right click on the newly restored virtual machine, select [Edit Settings].



3. For each virtual disk that was not restored, remove the corresponding [Hard disk] from [Hardware].



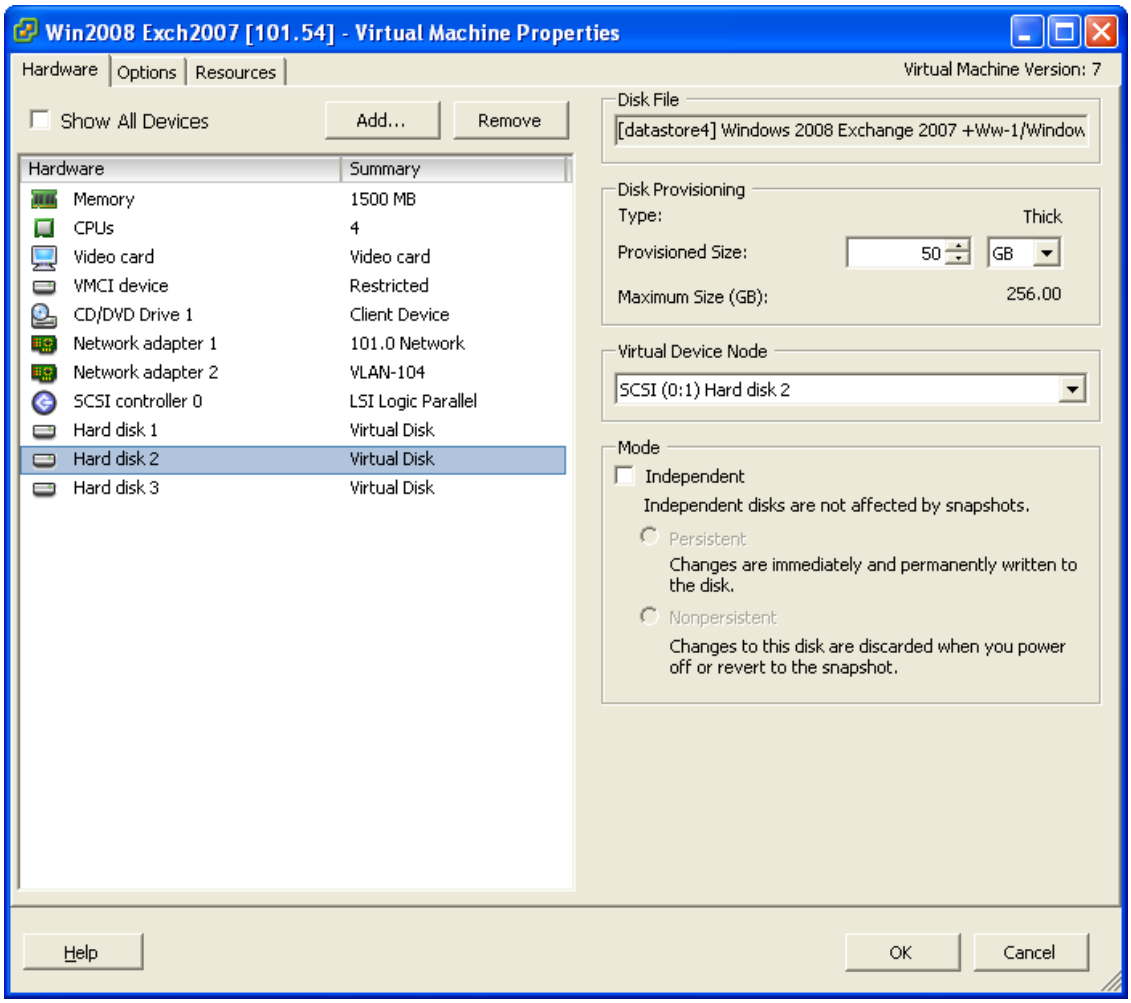
4. Start the virtual machine afterward.

For original virtual machine with snapshot

1. Open VMware vSphere Client.

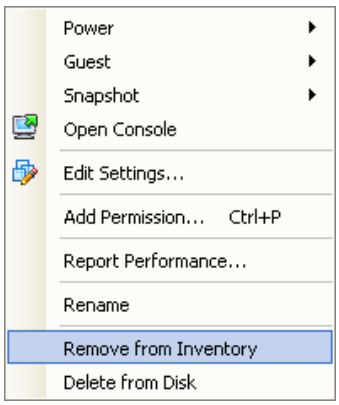
2. Under inventory, right click on the newly restored virtual machine, select [Edit Settings].

3. For each virtual disk that was not restored, remove the corresponding [Hard disk] from [Hardware].



4. Remove the VM from inventory.

   Right click on the newly restored virtual machine; select [Remove from Inventory].



5. Locate the virtual machine's folder location on the hypervisor.

   Important:
   Serious problem may occur if the configuration files are incorrectly modified; it may prevent the virtual machine from starting.

   Please only perform the following procedures if you have in-depth knowledge on VMware product.

6. Delete the lines of the removed virtual disk.

   - Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

   ```
   ${VM-Location}\${VM-Name}.vmsd
   ```

   - Locate the line of all non existing virtual disk.

   Example:

   Snapshot 1, SCSI (0:2) Disk 2 is removed.

```
.encoding = "UTF-8"
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
snapshot0.disk2.fileName = "Windows 2008-2.vmdk"
```

```
snapshot0.disk2.node = "scsi0:2"
```

- Remove the corresponding lines.

```
.encoding = "UTF-8"
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Perform the same steps for each snapshot.
- Save the changes afterward.

7. Update the number of virtual disk.

- Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

```
${VM-Location}\${VM-Name}.vmsd
```

- Locate the *numDisks* parameter.

Example:

Snapshot 1, if one of the disks is removed, updates the value of *snapshot0.numDisks*

```
.encoding = "UTF-8"
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
```

```
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Modify the line from:

snapshot0.numDisks = "3"

To

snapshot0.numDisks = "2"

```
.encoding = "UTF-8"
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "2"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Perform the same steps for each snapshot (e.g. *snapshot0.*, snapshot1.**).
- Save the changes afterward.

8. Add the VM back into the inventory.
9. Remove any existing snapshot.

   Important:
   The restored virtual machine does not support the reversion of previous snapshots if they contain virtual disks not restored.

10. Start the virtual machine.

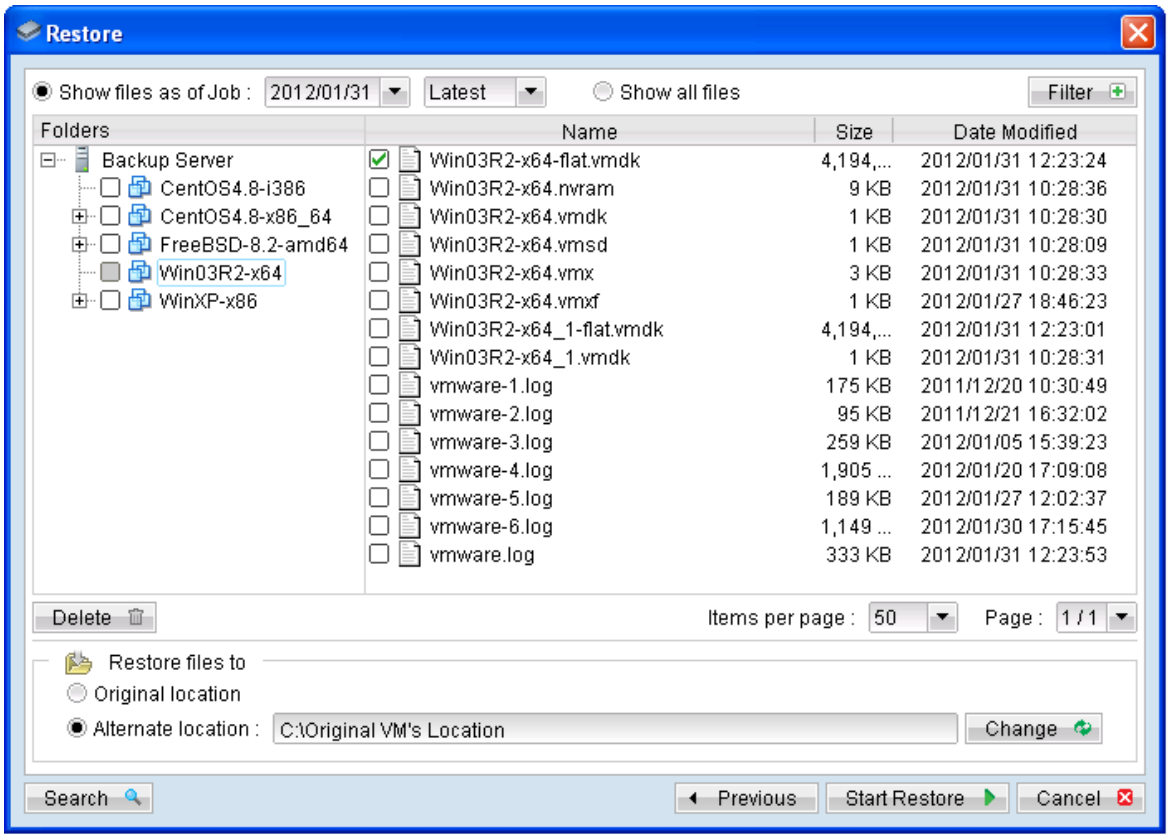
13.1.7 How to restore individual virtual disk

Individual virtual disk can be restored to the original VM, or to be added to a new VM.

13.1.1.7 How to restore individual virtual disk to the original VM

The procedure to restore individual virtual disk to the original VM is very similar to the procedure to restore virtual machine to a new hypervisor.

The main different is that user must select the restore to [Alternate location] option, and select the directory path to the original VM location.

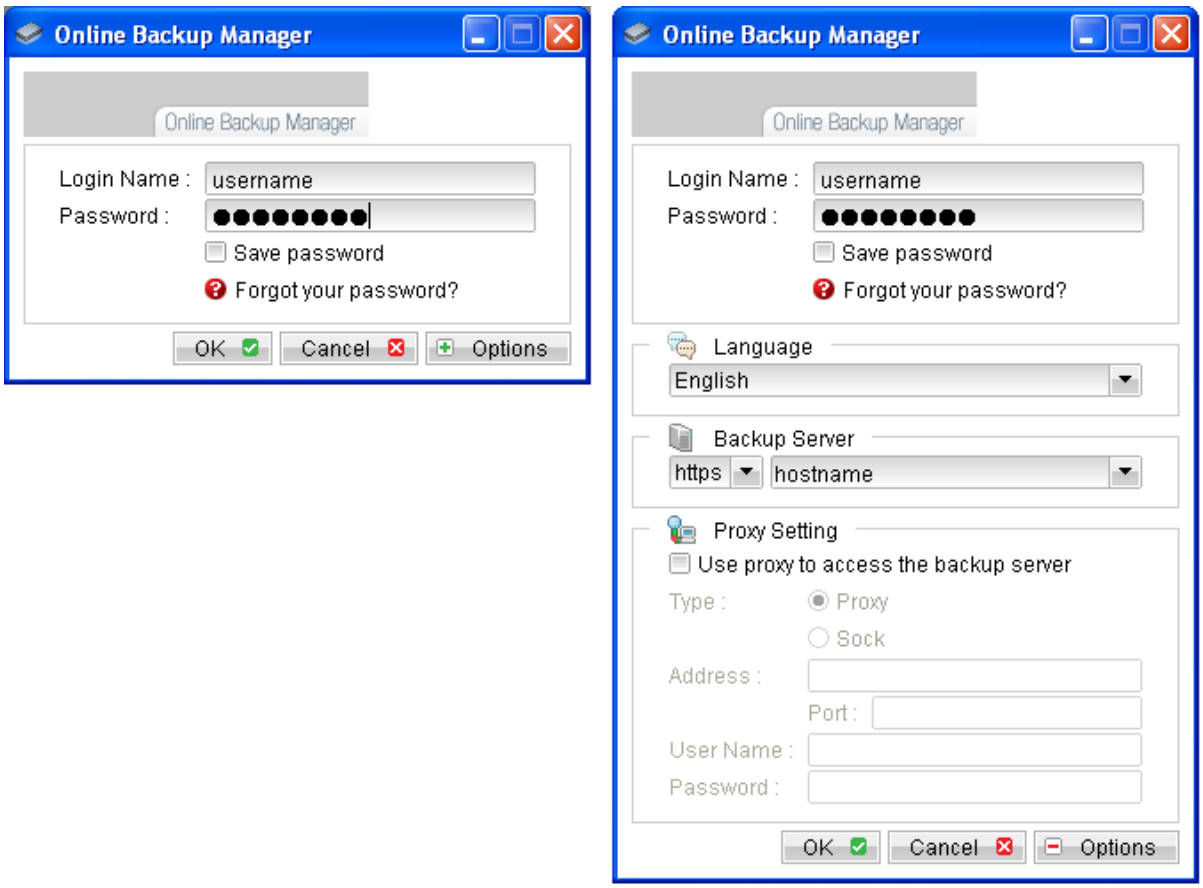


For full instructions, please refer to the above sections.

13.1.2.7 How to restore individual virtual disk to a different VM

1. Login to the backup application's user interface.

For backup client computer on Windows, double-click on the OBM desktop icon or right-click on the system tray icon:

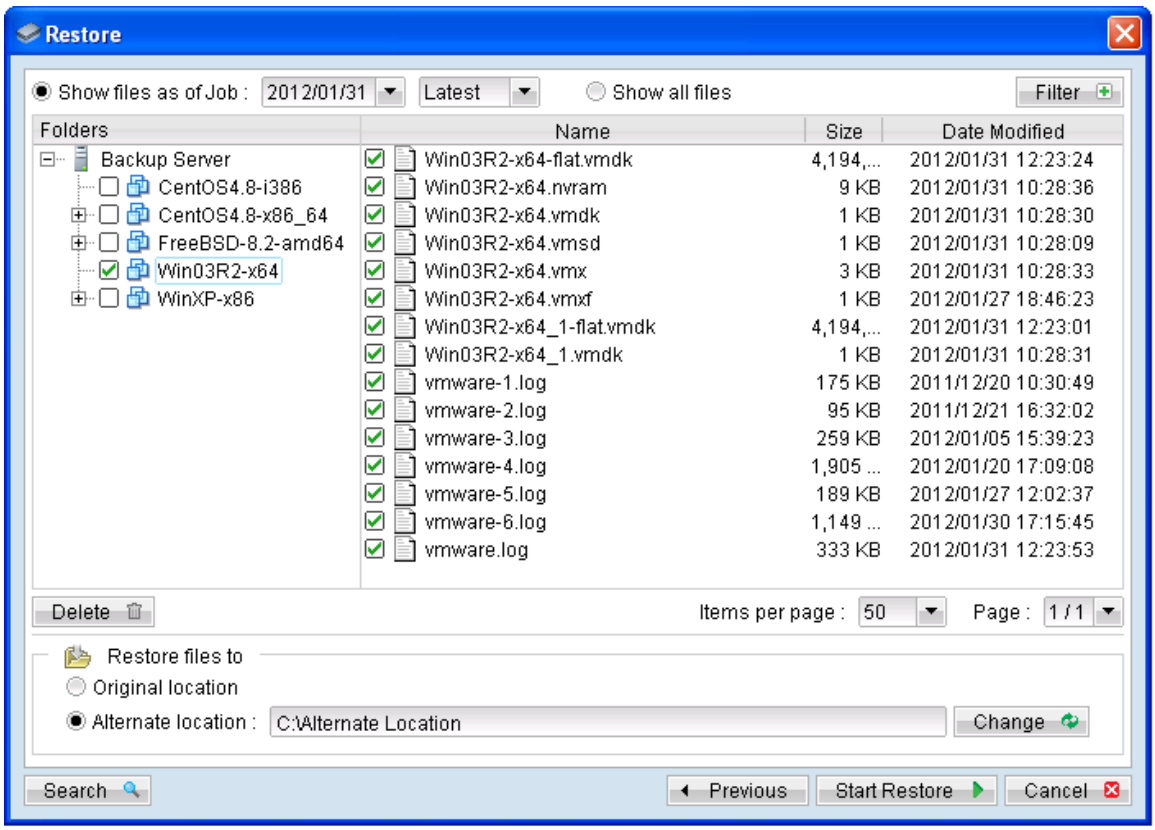


For backup client computer on Mac OS X, double-click on the OBM desktop icon.

For VMware Server installation on Linux, enter the following command to start the OBM graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Restore] button and the corresponding backup set.



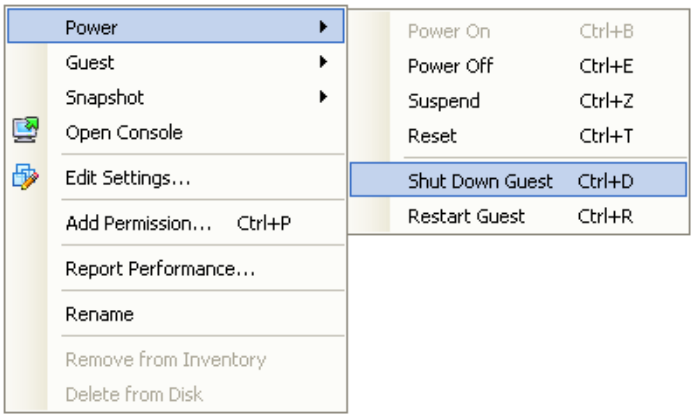
3. Select the virtual machines to be restored and choose [Alternate location] for restore files to.

4. Click on the [Change] button and browse to the directory path which you would like to restore the data to.

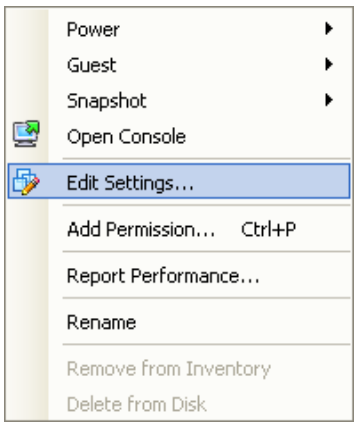
5. Click the [Start Restore] button to begin the restore process.

6. When the restore process is completed, open VMware vSphere Client.

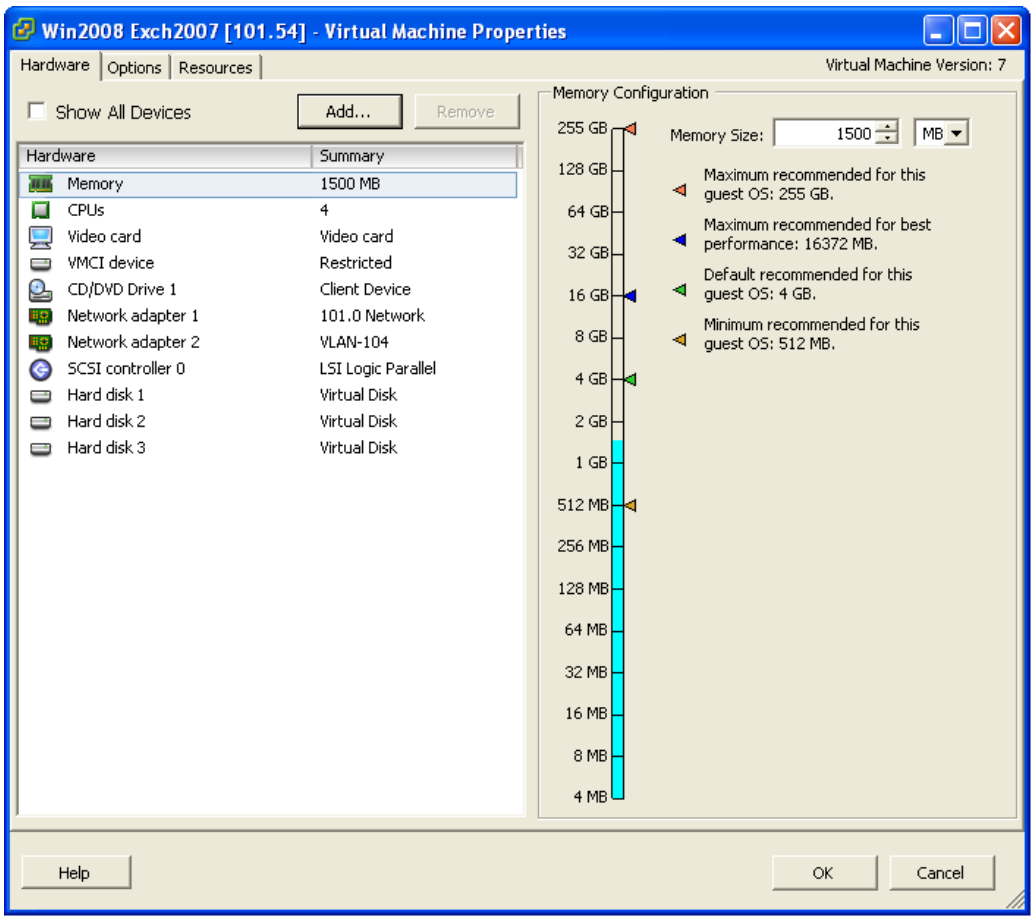
7. Under the inventory, powers down the corresponding virtual machine to be restored to.



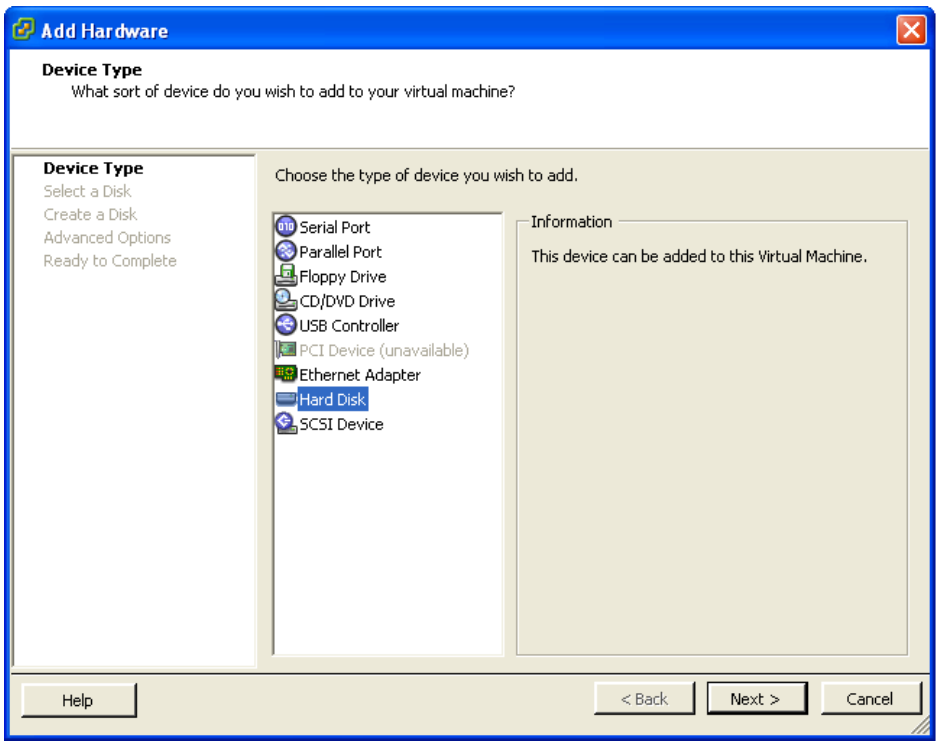
8. Right click on the corresponding VM, and select [Edit Settings].



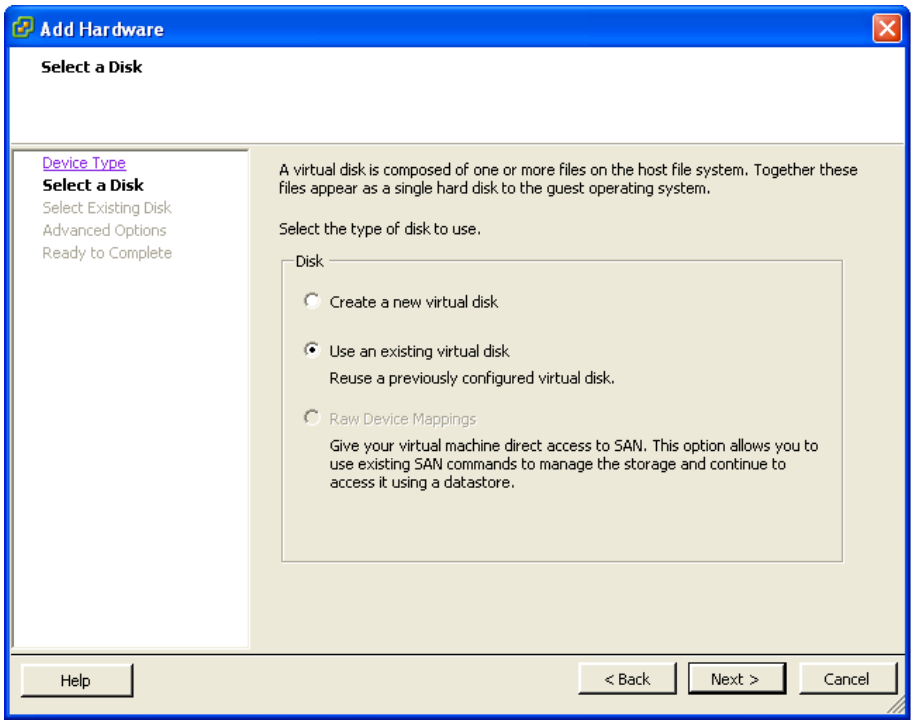
9. Select [Add] to add the newly restored virtual disk.



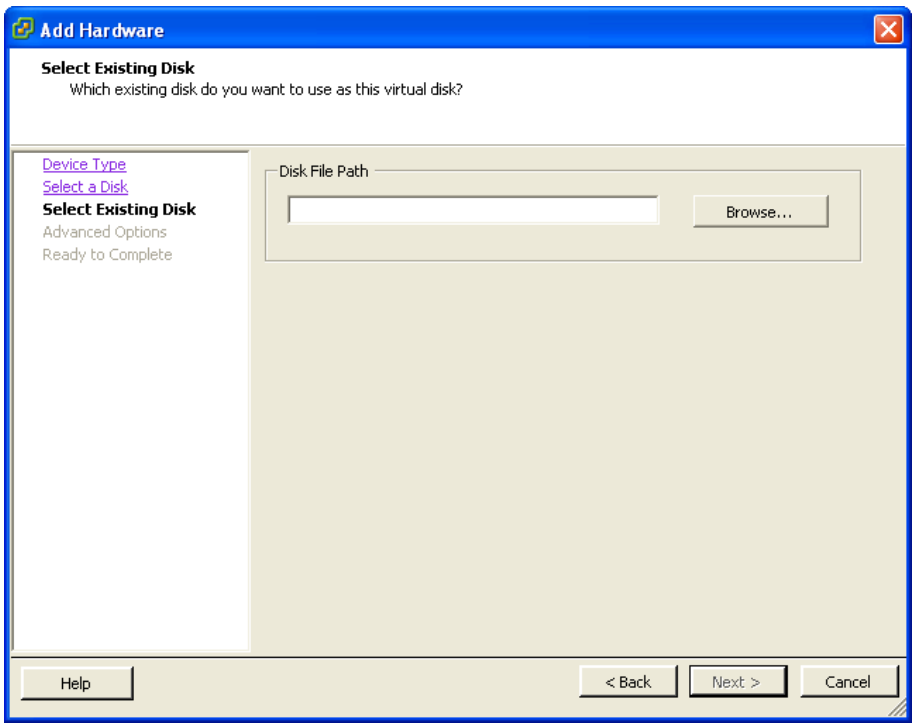
10. Select [Hard Disk] and then [Next].



11. Choose the option to [Use an existing virtual disk].


Add Hardware
Select a Disk
Device Type
Select a Disk
Select Existing Disk
Advanced Options
Ready to Complete
A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system.
Select the type of disk to use.
Disk
Create a new virtual disk
Use an existing virtual disk
Reuse a previously configured virtual disk.
Raw Device Mappings
Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.
Help
< Back
Next >
Cancel

12. Click [Browse] and browse to the newly restored virtual disk.



13. Follow the instruction provided in the [Add Hardware] menu.
14. Start the virtual machine.

13.2 Backup virtual machines running on VMware Server

13.2.1 Supported versions

The VMware VM backup module is supported for the following VMware Server versions:

- VMware Server 1.x
- VMware Server 2.x

For more details, please refer to Help Centre Article:
https://help..com/openArticle.aspx?aid=2323

13.2.2 Requirements and recommendations

Please ensure that the following requirements are met by the VMware Server:

1. OBM version 6.7 or above is installed on the VMware Server.

   Note:
   Resource allocation for both VM hosting and backup operation must be taken into consideration.

2. OBM must be installed on the hypervisor.

3. For VMware Server installation on Linux:

   - The root account must be enabled.
   - GUI environment must be installed on the hypervisor (e.g. GOME or KDE).

4. The following TCP ports must be opened on the hypervisor:

   - Port 902
   - Port 912
   - Port 8222
   - Port 8333

5. Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation.

6. It is recommended that the datastore have disk space of the largest sized virtual machine to be backed up.

7. It is recommended that the temporary directory have disk space of at least 50% of the largest sized virtual machine to be backed up.

8. It is recommended that the temporary directory be configured on a local drive.

9. It is recommended that the temporary directory is not configured on the same partition which the operating system is installed on.

10. Consider performing routine recovery test to ensure your backup is setup and performed properly.

13.2.3 Limitations

The following are limitations of the VMware VM backup module:

1. For VMware Server 1.x, active virtual machine selected for backup must be powered down for the backup process to begin.

2. For backup of individual virtual disk, the restored virtual machine does not support the reversion of previous snapshots, if the snapshot contains disks which are not previously backed up by OBM.

3. Independent Disk is not supported. For virtual machines with Independent Disks, those disks will not be backed up.

13.2.4 Overview

The following steps are performed during a backup job:

1. Connection from the backup client to the backup server is established.

2. Download the server file list from the backup server.

3. VMware Server 1.x
   Commands are issued to the hypervisor to shutdown the virtual machine for backup.

   VMware Server 2.x
   Commands are issued to the hypervisor to create snapshot of the virtual machine for backup.

4. Server and local file lists are compared to determine which file will be uploaded.

5. Delta file is generated for modified file (if necessary).

6. Existing, and snapshot data are encrypted, compressed, and streamed to the backup server.

7. VMware Server 1.x
   Commands are issued to the hypervisor to start up the virtual machine.

   VMware Server 2.x

Commands are issued to the hypervisor to create snapshot of the virtual machine for backup.

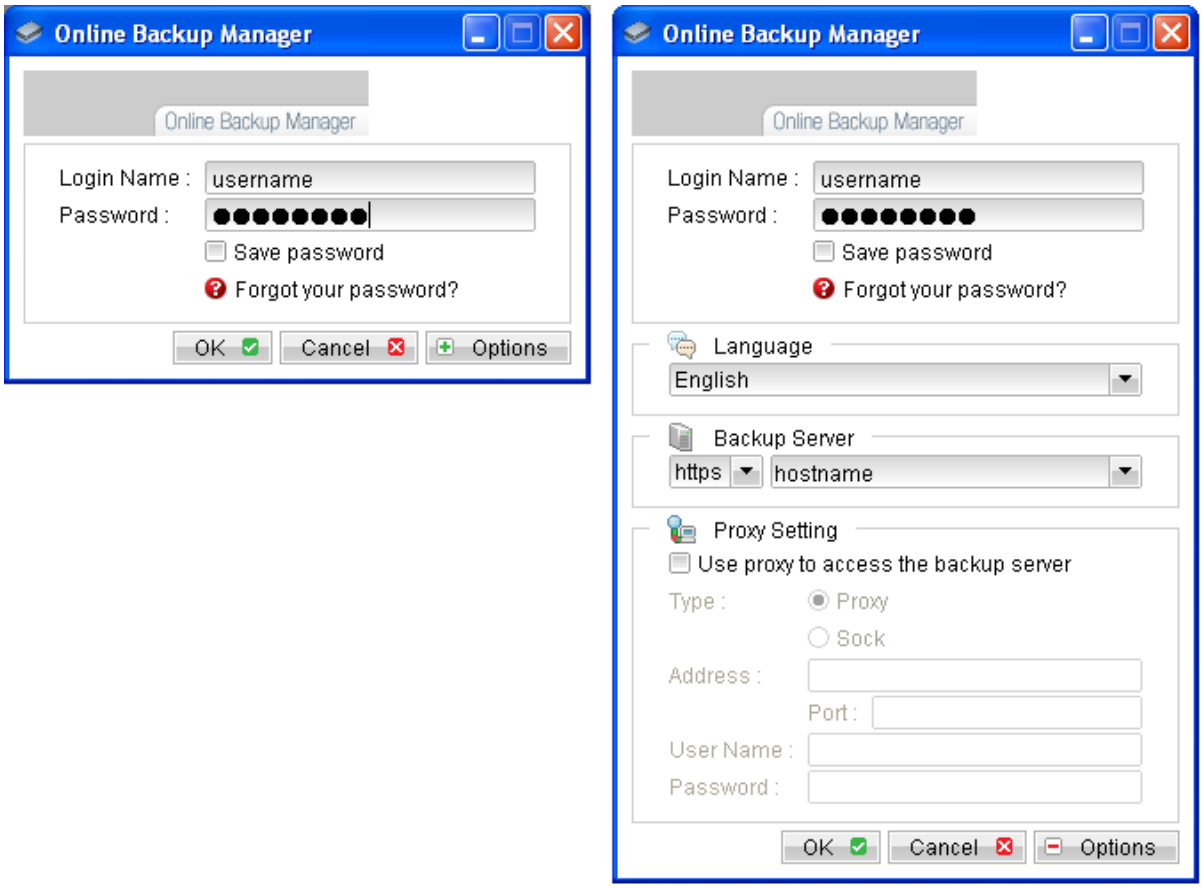
8. Backup completed successfully.

13.2.5 How to backup virtual machines on VMware Server

Refer to the following instructions to backup VM running on VMware Server:

1. Login to the backup application's user interface.

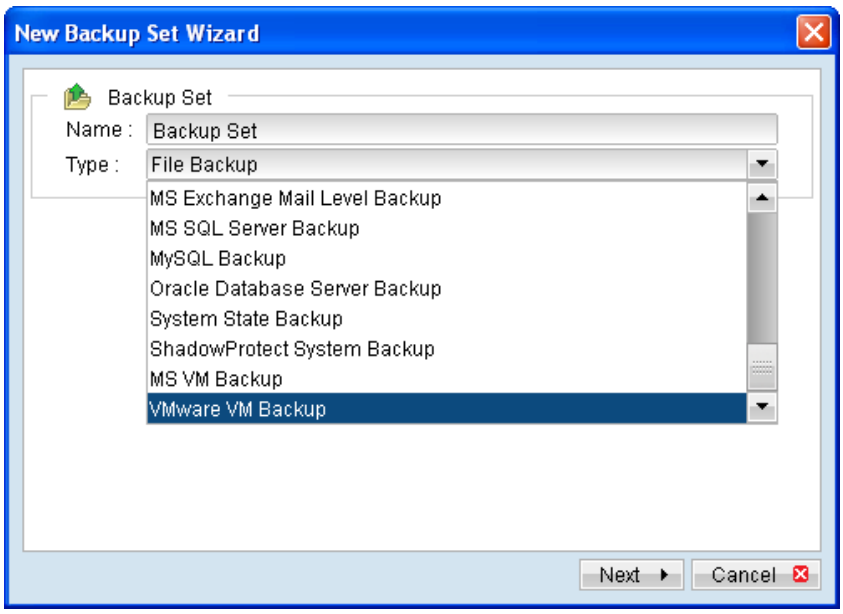
For VMware Server installation on Windows, double-click on the OBM desktop icon or right-click on the system tray icon:



For VMware Server installation on Linux, enter the following command to start the OBM graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.



3. Create a VMware VM Backup set by selecting [VMware VM Backup] from the backup set type dropdown menu.

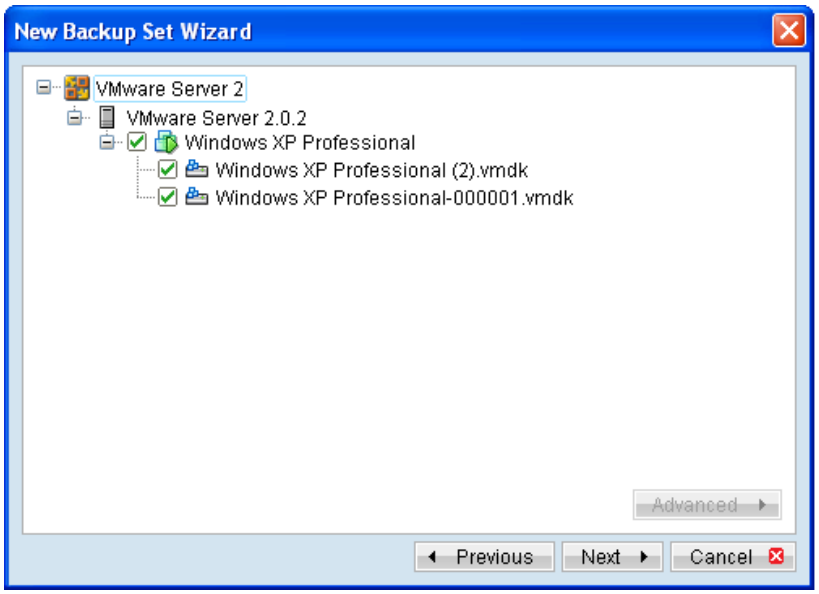
4. Enter the corresponding information required:

Menu Items	Description
Name	Enter a backup set name of your choice.
Type	Select backup set type [VMware VM Backup].
VMware Host Version	Select host version, for example [VMware Server 1] or [VMware Server 2]
Username	Enter the username of the hypervisor administrator.
Password	Enter the password of the hypervisor administrator.
Host	Default to 127.0.0.1, OBM must be installed on the

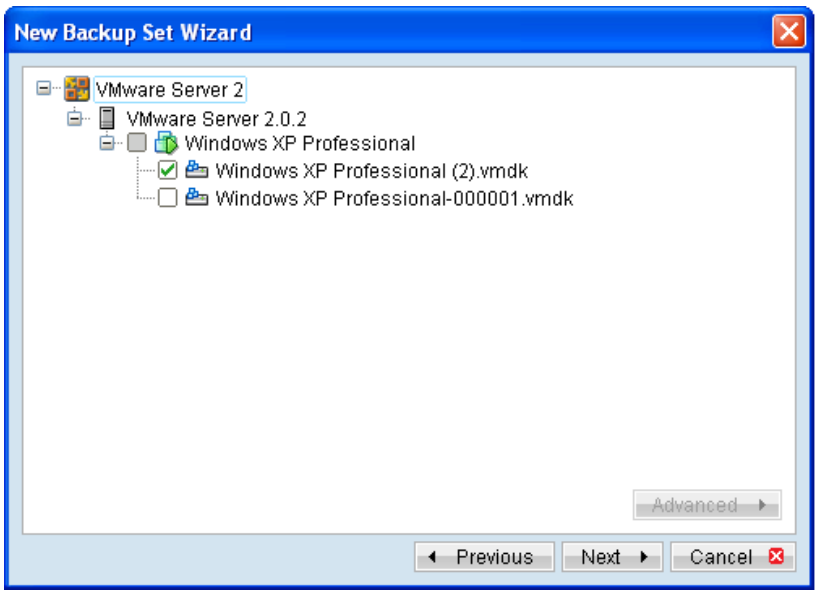
	hypervisor.
Port	Enter the corresponding port to the hypervisor.

5. Select [Next] to proceed.

6. Select the corresponding virtual machines for backup.



7. Alternatively, select individual virtual disk for backup by expanding the corresponding VM sub tree.



Important:
For backup of VM with snapshot, backup of the whole VM instead of individual disk is highly recommended.

8. Configure a backup schedule for unattended backups.

Note:
Multiple backup schedules of different types can be configured for the same backup set.

9. Select an encryption setting for your backup set.

10. Press the [OK] button to complete the configuration of backup set.

11. Scheduled backup will run automatically at the configured schedule time.

12. Click [Backup] button on the left panel to perform a backup immediately.

Note:
For VMware Server 1.x, active virtual machine (selected for backup) must be powered down for the backup process to begin.

13.2.6 How to restore virtual machines on VMware Server

Refer to the following instructions to restore VM running on VMware Server.

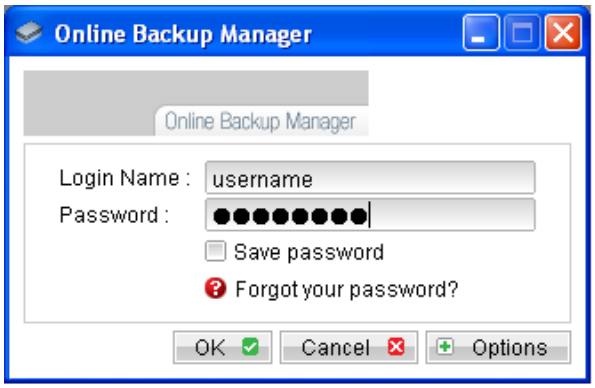
VM can be restored to the original location with the following condition:

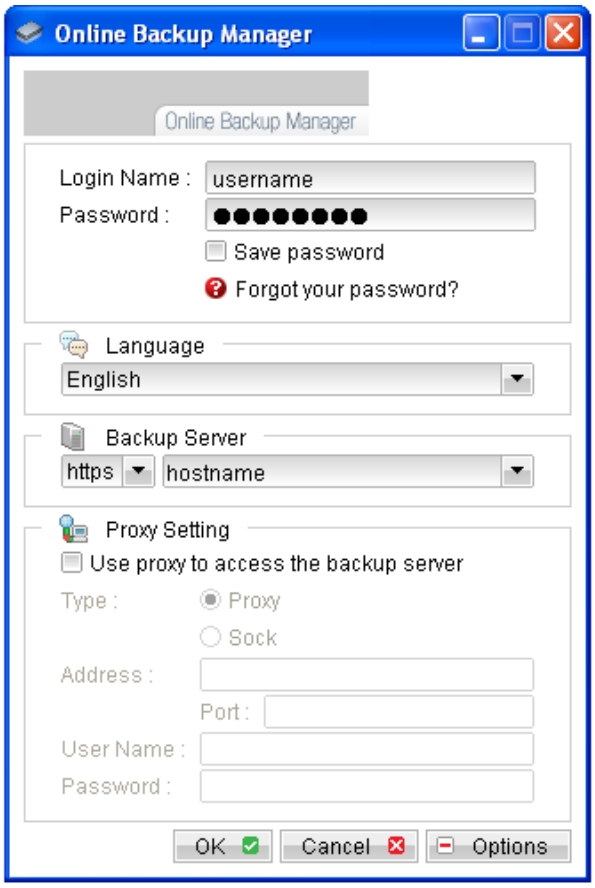
- If the VM to be restored does not exist on the original hypervisor, the VM will be restored as a new virtual machine.
- If the VM to be restored still exist on the original hypervisor, the existing VM will be replaced by the backed up version.

13.2.1.6 How to restore virtual machines to the original hypervisor

1. Login to the backup application's user interface.

For VMware Server installation on Windows, double-click on the OBM desktop icon or right-click on the system tray icon:

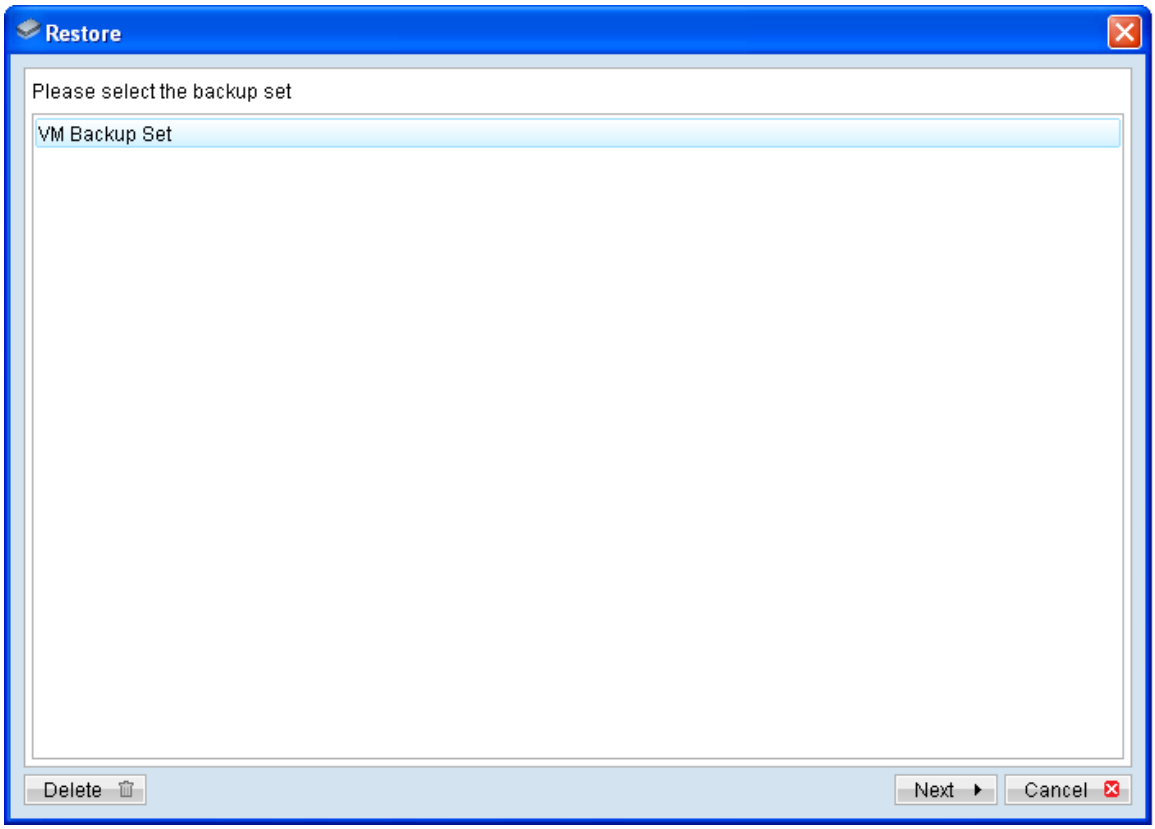




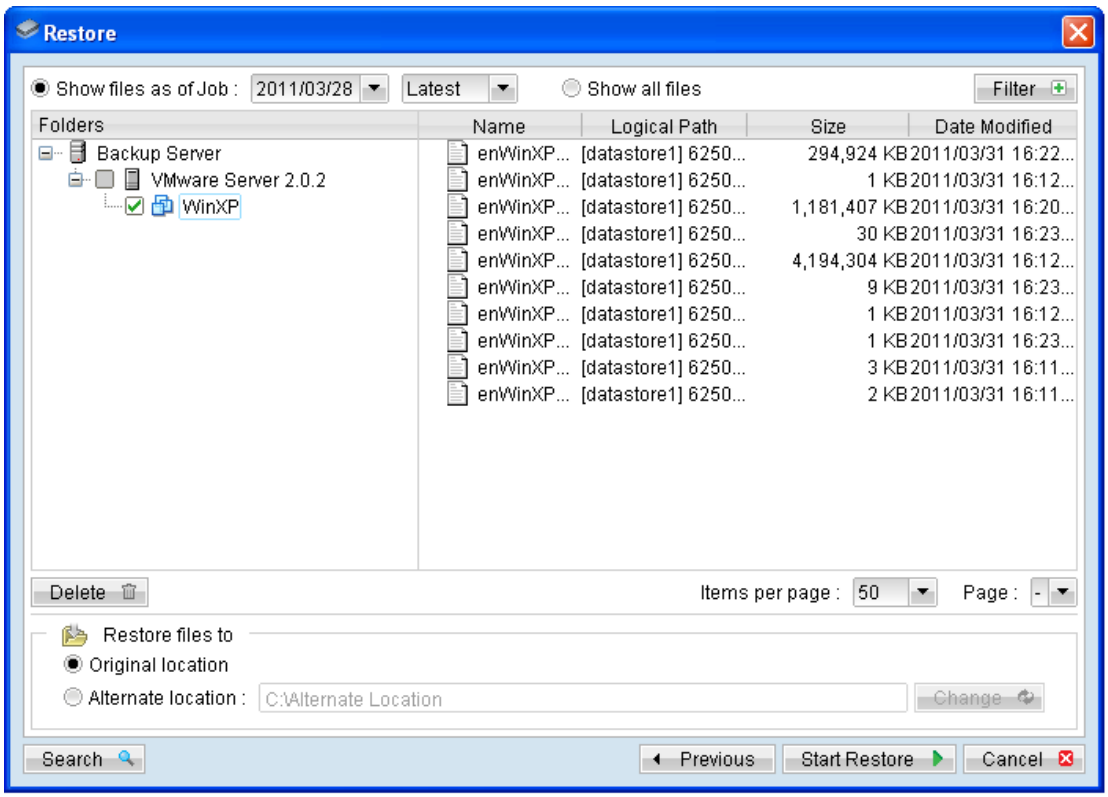
For VMware Server installation on Linux, enter the following command to start the OBM graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Restore] button and the corresponding backup set.

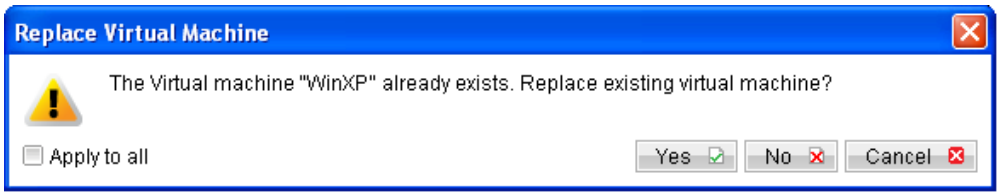


3. Select the virtual machines to be restored and choose [Original Location] for restore files to.



4. Click the [Start Restore] button to begin the restore process.

5. User will be prompted if a virtual machine selected to be restored exist on the hypervisor.



6. When the restore process is completed, the virtual machines will be restored to the original hypervisor.

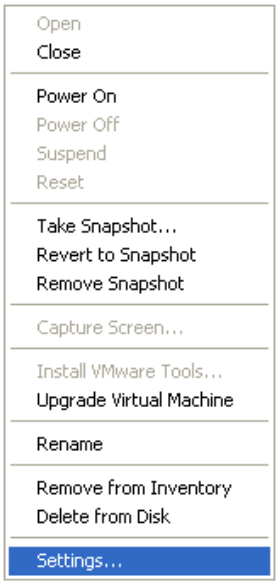
7. For any virtual disk that was not restored (e.g. original backup source did not include all hard disks configured for the VM).

   Continue to the next steps for instruction to remove the missing hard disk from the virtual machine's configuration.

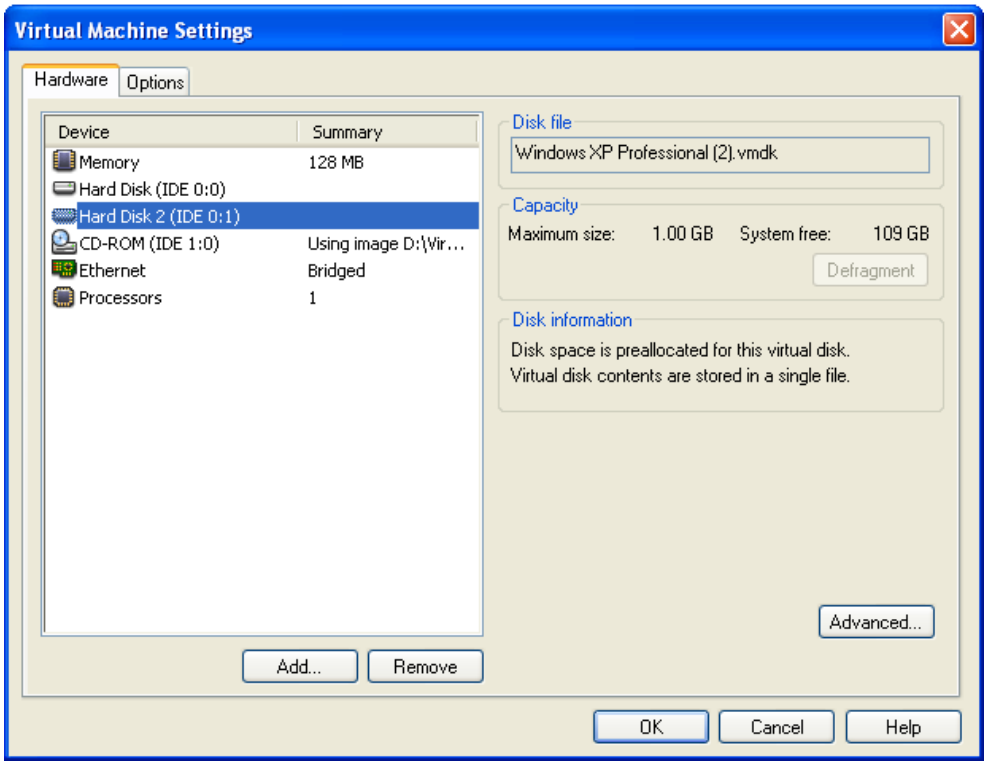
For original virtual machine with no snapshot

1. Open VMware Server Console.

2. Under inventory, right click on the newly restored virtual machine, select [Settings].



3. For each virtual disk that was not restored, remove the corresponding [Hard disk] from [Hardware].

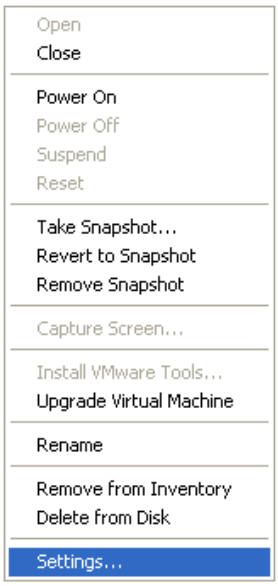


4. Start the virtual machine afterward.

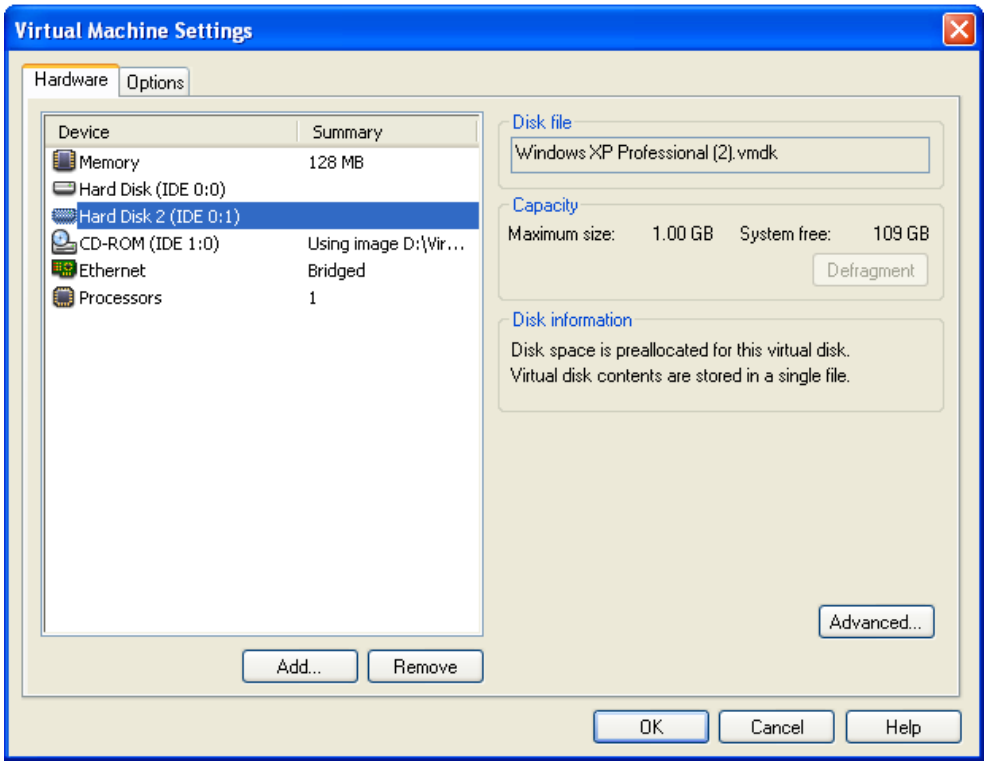
For original virtual machine with snapshot

1. Open VMware Server Console.

2. Under inventory, right click on the newly restored virtual machine, select [Settings].

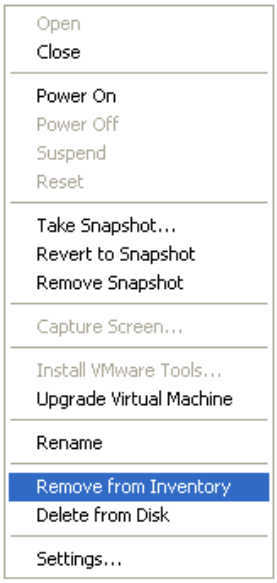


3. For each virtual disk that was not restored, remove the corresponding [Hard disk] from [Hardware].



4. Remove the VM from inventory.

5. Right click on the newly restored virtual machine; select [Remove from Inventory].



6. Locate the virtual machine's folder location on the hypervisor.

   Important:
   Serious problem may occur if the configuration files are incorrectly modified; it may prevent the virtual machine from starting.

   Please only perform the following procedures if you have in-depth knowledge on VMware product.

7. Delete the lines of the removed virtual disk.

   - Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

   ```
   ${VM-Location}\${VM-Name}.vmsd
   ```

   - Locate the line of all non existing virtual disk.

   Example:

   Snapshot 1, SCSI (0:2) Disk 2 is removed.

   ```
   snapshot.lastUID = "1"
   snapshot.numSnapshots = "1"
   snapshot.current = "1"
   snapshot0.uid = "1"
   snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
   snapshot0.displayName = "Snapshot1"
   snapshot0.description = ""
   snapshot0.createTimeHigh = "309233"
   snapshot0.createTimeLow = "1291281261"
   snapshot0.numDisks = "3"
   snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
   ```

```
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
snapshot0.disk2.fileName = "Windows 2008-2.vmdk"
snapshot0.disk2.node = "scsi0:2"
```

- Remove the corresponding lines.

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Perform the same steps for each snapshot.
- Save the changes afterward.

8. Update the number of virtual disk.

- Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

```
${VM-Location}\${VM-Name}.vmsd
```

- Locate the *numDisks* parameter.

Example:

Snapshot 1, if one of the disks is removed, updates the value of *snapshot0.numDisks*

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
```

```
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Modify the line from:

snapshot0.numDisks = "3"

To

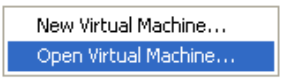
snapshot0.numDisks = "2"

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "2"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

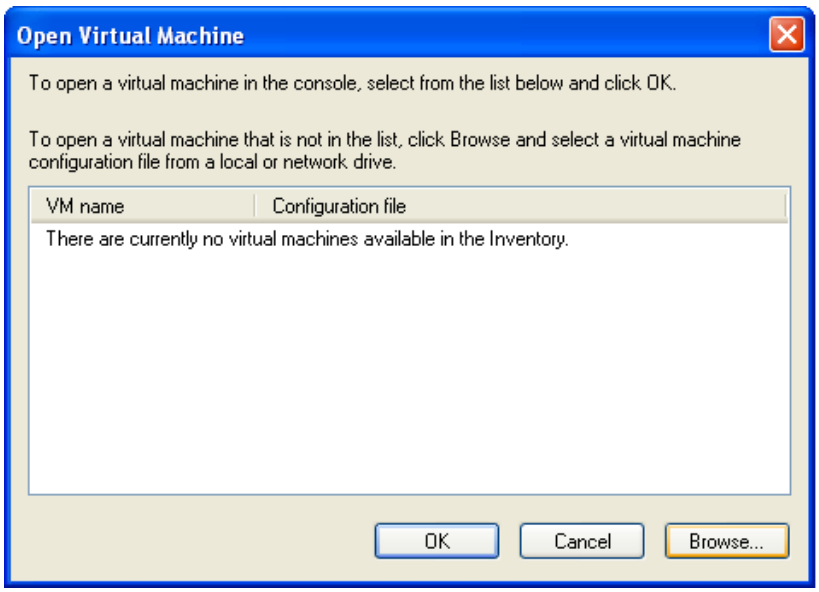
- Perform the same steps for each snapshot.
- Save the changes afterward.

9. Add the VM back into the inventory.

   Right click on the Inventory; select [Open Virtual Machine].



10. Browse to the corresponding *${VM-Name}.vmx* file.


Open Virtual Machine
To open a virtual machine in the console, select from the list below and click OK.
To open a virtual machine that is not in the list, click Browse and select a virtual machine configuration file from a local or network drive.
VM name
Configuration file
There are currently no virtual machines available in the Inventory.
OK
Cancel
Browse...

11. Remove any existing snapshot.

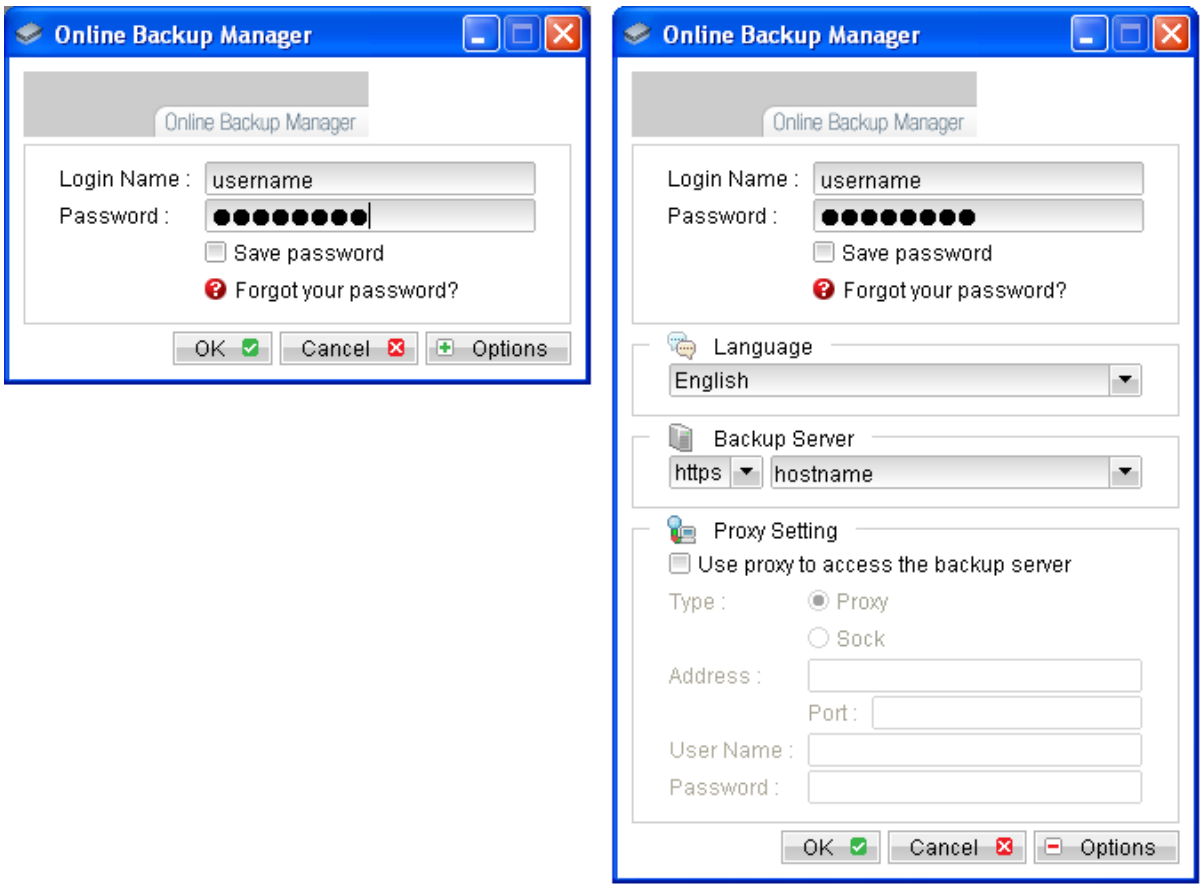
    Important:
    The restored virtual machine does not support the reversion of previous snapshots if they contain virtual disks not restored.

12. Start the virtual machine.

13.2.2.6 How to restore virtual machines to another hypervisor

1. Login to the backup application's user interface.

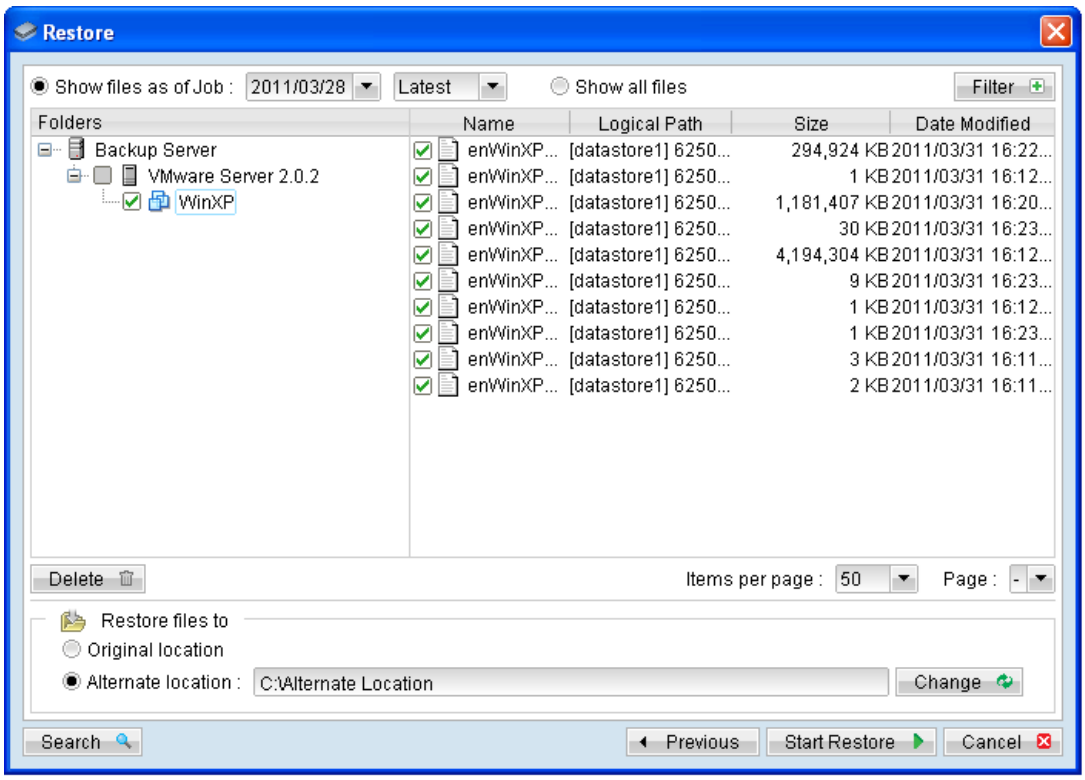
For VMware Server installation on Windows, double-click on the OBM desktop icon or right-click on the system tray icon:



For VMware Server installation on Linux, enter the following command to start the OBM graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Restore] button and the corresponding backup set.



3. Select the virtual machines to be restored and choose [Alternate location] for restore files to.

4. Click on the [Change] button and browse to the directory path which you would like to restore the data to.

5. Click the [Start Restore] button to begin the restore process.

6. When the restore process is completed, data of the selected virtual machines will be restored to the specified location.

7. Register the virtual machines on the new hypervisor.

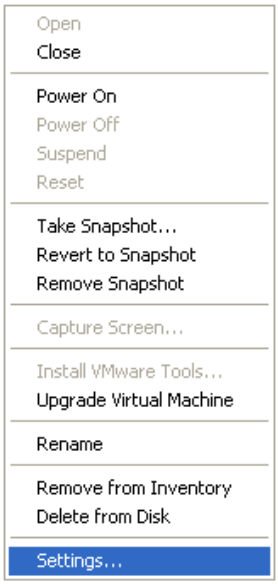
8. For any virtual disk that was not restored (e.g. original backup source did not include all hard disks configured for the VM).

   Continue to the next steps for instruction to remove the missing hard disk from the virtual machine's configuration.

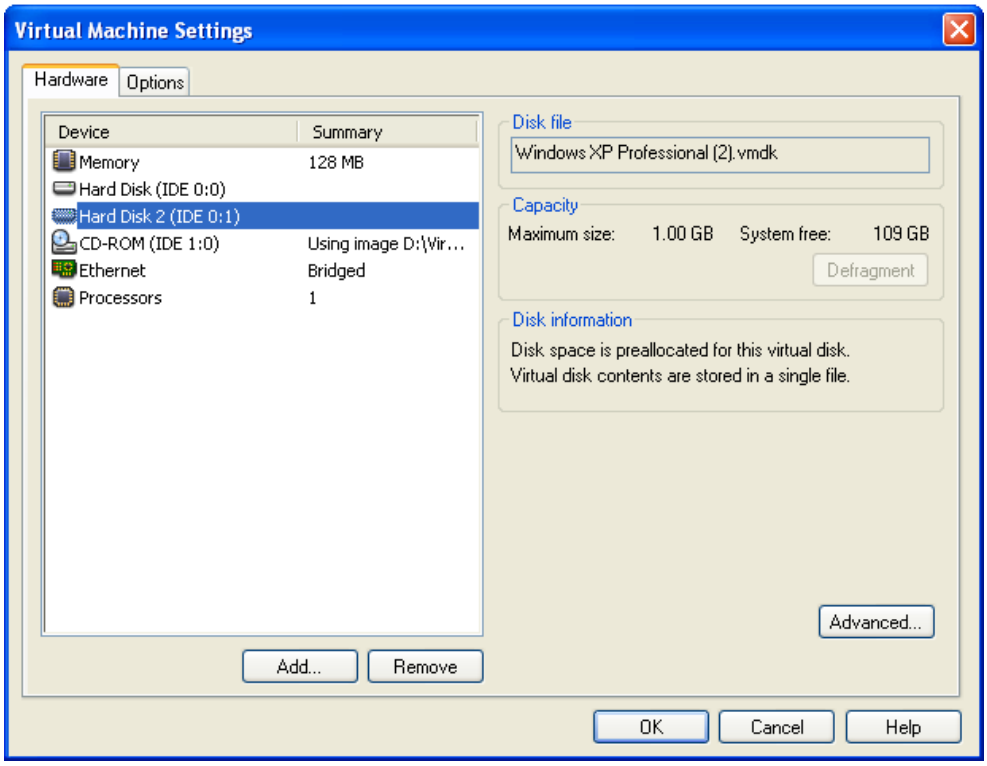
For original virtual machine with no snapshot

1. Open VMware Server Console.

2. Under inventory, right click on the newly restored virtual machine, select [Settings].



3. For each virtual disk that was not restored, remove the corresponding [Hard disk] from [Hardware].

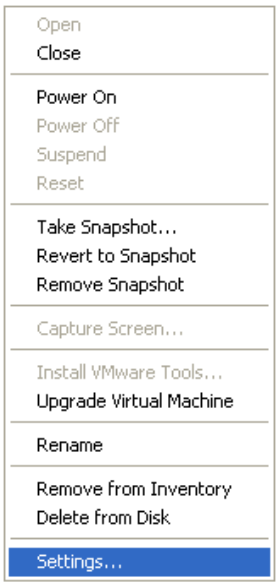


4. Start the virtual machine afterward.

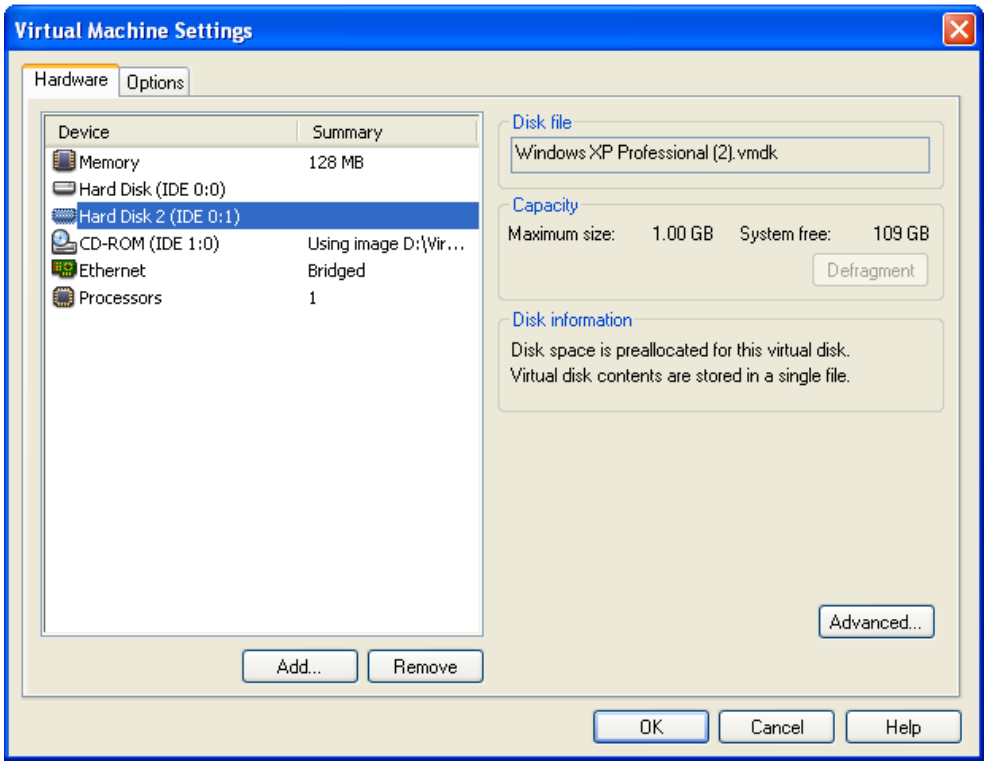
For original virtual machine with snapshot

1. Open VMware Server Console.

2. Under inventory, right click on the newly restored virtual machine, select [Settings].

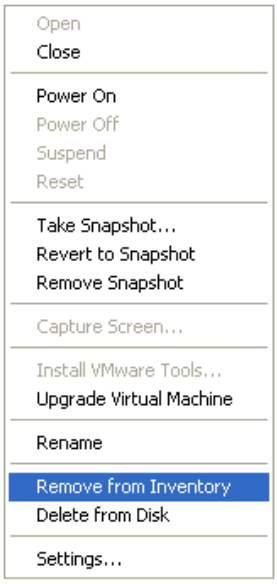


3. For each virtual disk that was not restored, remove the corresponding [Hard disk] from [Hardware].



4. Remove the VM from inventory.

5. Right click on the newly restored virtual machine; select [Remove from Inventory].



6. Locate the virtual machine's folder location on the hypervisor.

   Important:
   Serious problem may occur if the configuration files are incorrectly modified; it may prevent the virtual machine from starting.

   Please only perform the following procedures if you have in-depth knowledge on VMware product.

7. Delete the lines of the removed virtual disk.

   - Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

   ```
   ${VM-Location}\${VM-Name}.vmsd
   ```

   - Locate the line of all non existing virtual disk.

   Example:

   Snapshot 1, SCSI (0:2) Disk 2 is removed.

   ```
   snapshot.lastUID = "1"
   snapshot.numSnapshots = "1"
   snapshot.current = "1"
   snapshot0.uid = "1"
   snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
   snapshot0.displayName = "Snapshot1"
   snapshot0.description = ""
   snapshot0.createTimeHigh = "309233"
   snapshot0.createTimeLow = "1291281261"
   snapshot0.numDisks = "3"
   snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
   ```

```
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
snapshot0.disk2.fileName = "Windows 2008-2.vmdk"
snapshot0.disk2.node = "scsi0:2"
```

- Remove the corresponding lines.

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Perform the same steps for each snapshot.
- Save the changes afterward.

8. Update the number of virtual disk.

- Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

```
${VM-Location}\${VM-Name}.vmsd
```

- Locate the *numDisks* parameter.

Example:

Snapshot 1, if one of the disks is removed, updates the value of *snapshot0.numDisks*

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
```

```
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Modify the line from:

snapshot0.numDisks = "3"

To

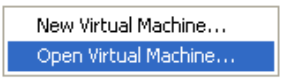
snapshot0.numDisks = "2"

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "2"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

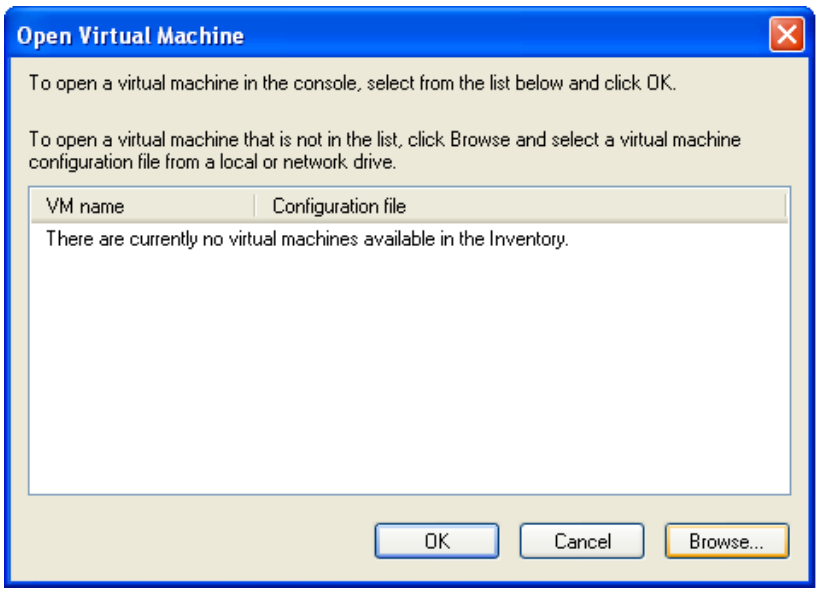
- Perform the same steps for each snapshot.
- Save the changes afterward.

9. Add the VM back into the inventory.

   Right click on the Inventory; select [Open Virtual Machine].



10. Browse to the corresponding *${VM-Name}.vmx* file.


Open Virtual Machine
To open a virtual machine in the console, select from the list below and click OK.
To open a virtual machine that is not in the list, click Browse and select a virtual machine configuration file from a local or network drive.
VM name
Configuration file
There are currently no virtual machines available in the Inventory.
OK
Cancel
Browse...

11. Remove any existing snapshot.

    Important:
    The restored virtual machine does not support the reversion of previous snapshots if they contain virtual disks not restored.

12. Start the virtual machine.

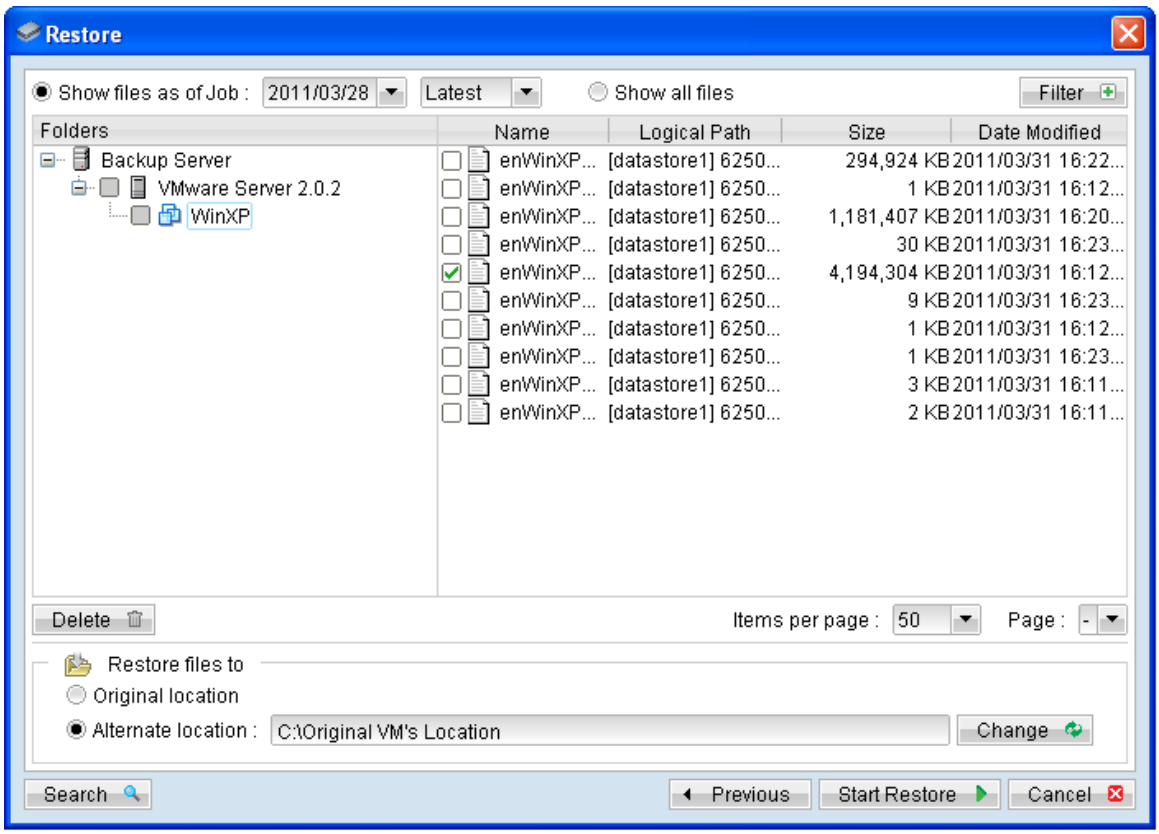
13.2.7 How to restore individual virtual disk

Individual virtual disk can be restored to the original VM, or to be added to a new VM.

13.2.1.7 How to restore individual virtual disk to the original VM

The procedure to restore individual virtual disk to the original VM is very similar to the procedure to restore virtual machine to a new hypervisor.

The main different is that user must select the restore to [Alternate location] option, and select the directory path to the original VM location.

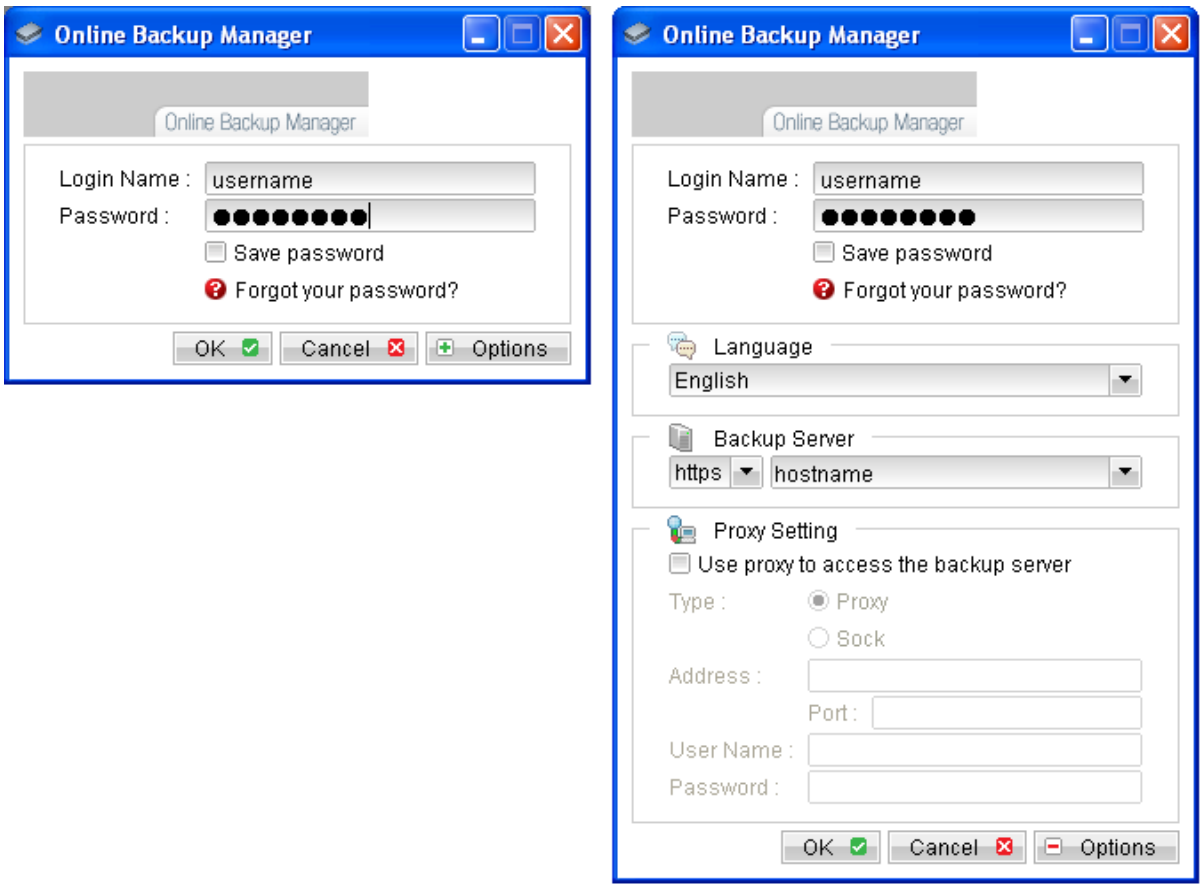


For full instructions, please refer to the above sections.

13.2.2.7 How to restore individual virtual disk to a different VM

1. Login to the backup application's user interface.

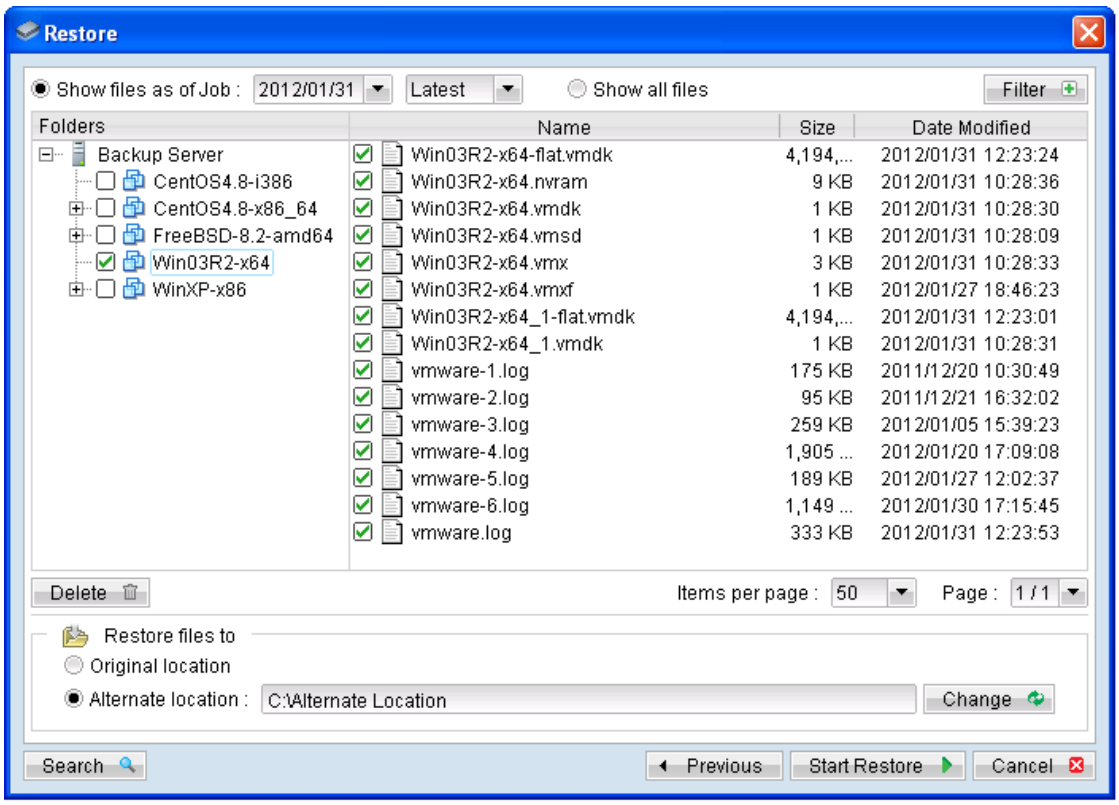
For VMware Server installation on Windows, double-click on the OBM desktop icon or right-click on the system tray icon:



For VMware Server installation on Linux, enter the following command to start the OBM graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Restore] button and the corresponding backup set.



3. Select the virtual machines to be restored and choose [Alternate location] for restore files to.

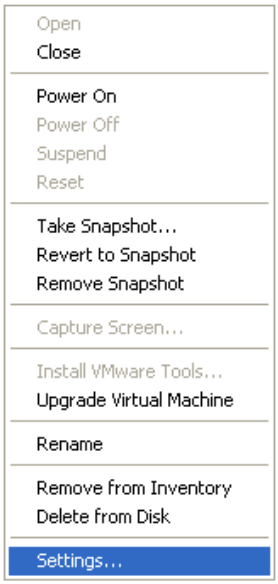
4. Click on the [Change] button and browse to the directory path which you would like to restore the data to.

5. Click the [Start Restore] button to begin the restore process.

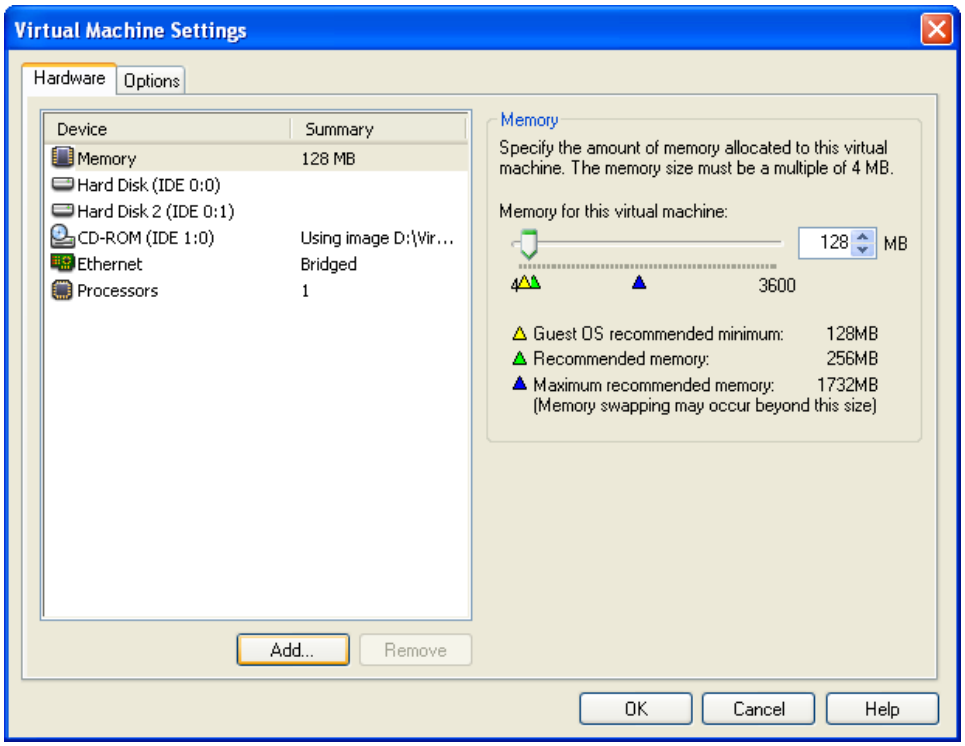
6. When the restore process is completed, open VMware Server Console.

7. Under the inventory, powers down the corresponding virtual machine to be restored to.

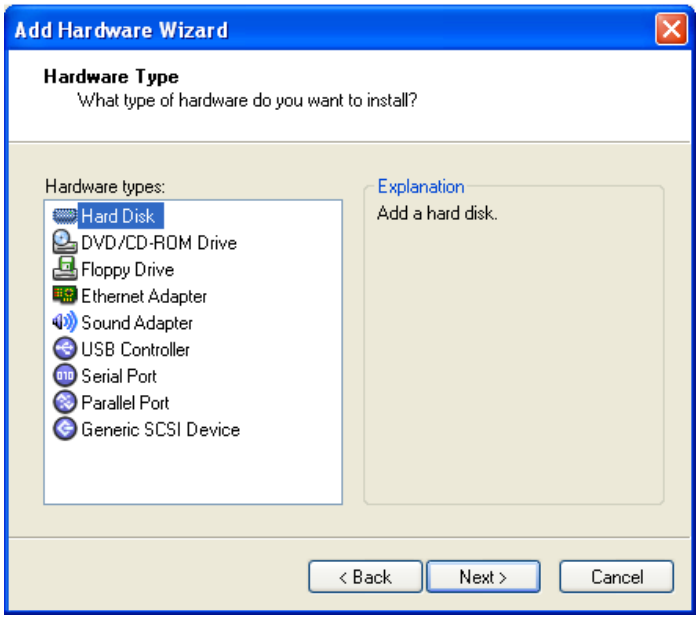
8. Right click on the corresponding VM, and select [Settings].



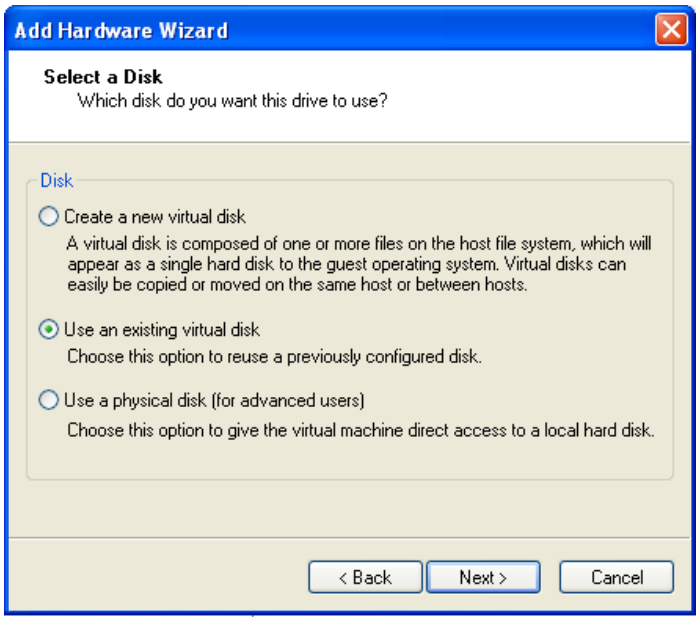
9. Select [Add] to add the newly restored virtual disk.



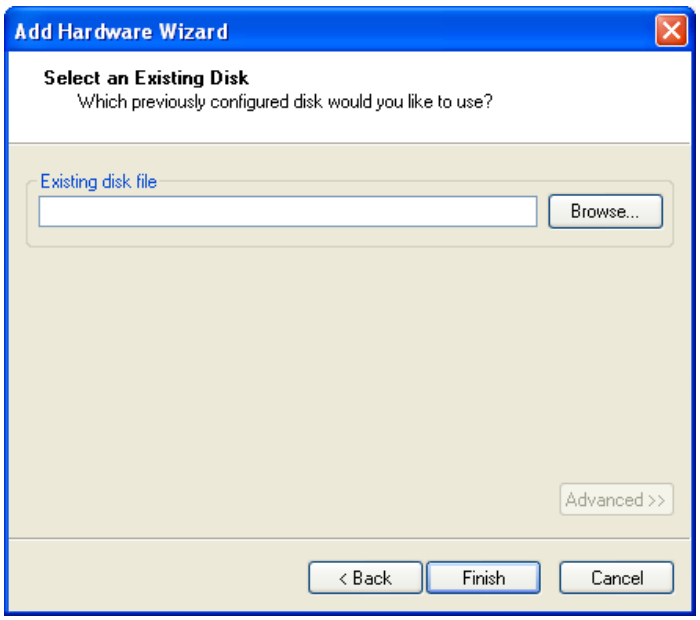
10. Select [Hard Disk] and then [Next].



11. Choose the option to [Use an existing virtual disk].


Add Hardware Wizard
Select a Disk
Which disk do you want this drive to use?
Disk
Create a new virtual disk
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
Use an existing virtual disk
Choose this option to reuse a previously configured disk.
Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk.
< Back
Next >
Cancel

12. Click [Browse] and browse to the newly restored virtual disk.



13. Follow the instruction provided in the [Add Hardware] wizard.
14. Start the virtual machine.

13.3 Backup virtual machines running on VMware Fusion

13.3.1 Supported versions

The VMware VM backup module is supported for the following VMware Fusion version:

- VMware Fusion 3
- VMware Fusion 4

For more details, please refer to Help Centre Article:
https://help..com/openArticle.aspx?aid=2323

13.3.2 Requirements and recommendations

Please ensure that the following requirements are met by the VMware Fusion machine:

1. OBM version 6.7 or above is installed.

   Note:
   Resource allocation for both VM hosting and backup operation must be taken into consideration.

2. OBM is installed on the VM Fusion machine.

3. For VMware Fusion 4, the application bundle must be located under */Applications*.

   ```
   /Applications/VMware Fusion.app/Contents/Library
   ```

   Otherwise, please move the application bundle to */Applications*.

4. Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation.

5. It is recommended that the datastore have disk space of the largest sized virtual machine to be backed up.

6. It is recommended that the temporary directory have disk space of at least 50% of the largest sized virtual machine to be backed up.

7. It is recommended that the temporary directory be configured on a local drive.

8. It is recommended that the temporary directory is not configured on the same partition which the operating system is installed on.

9. Consider performing routine recovery test to ensure your backup is setup and performed properly.

13.3.3 Limitations

The following are limitations of the VMware VM backup module:

1. Boot Camp virtual machine is not supported.

2. For backup of individual virtual disk, the restored virtual machine does not support the reversion of previous snapshots, if the snapshot contains disks which are not previously backed up by OBM.

3. Independent Disk is not supported. For virtual machines with Independent Disks, those disks will not be backed up.

13.3.4 Overview

The following steps are performed during a backup job:

1. Connection from the backup client to the backup server is established.

2. Download the server file list from the backup server.

3. Commands are issued to the hypervisor to create snapshot of the virtual machine for backup.

4. Server and local file lists are compared to determine which file will be uploaded.

5. Delta file is generated for modified file (if necessary).

6. Existing, and snapshot data are encrypted, compressed, and streamed to the backup server.

7. Commands are issued to the hypervisor to remove snapshot created for backup.

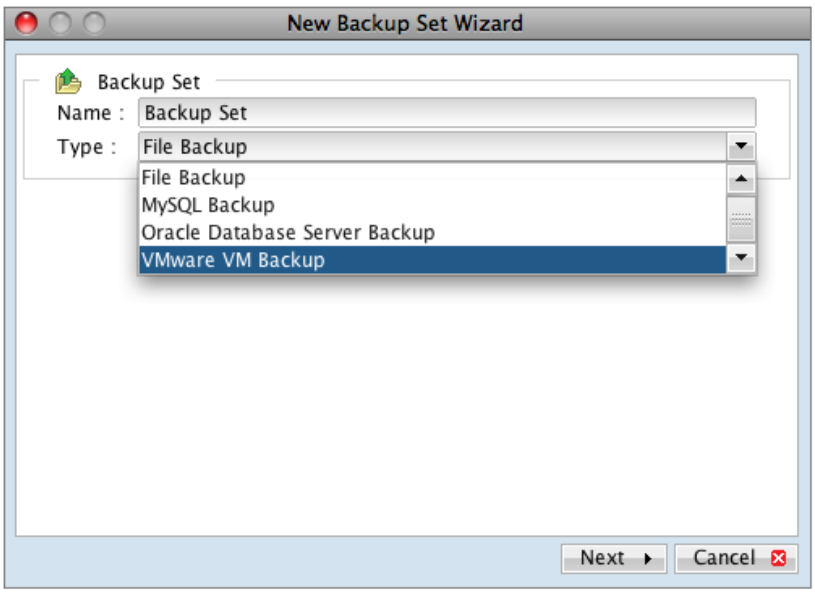
8. Backup completed successfully.

13.3.5 How to backup virtual machines on VMware Fusion

Refer to the following instructions to backup VM running on VMware Fusion:

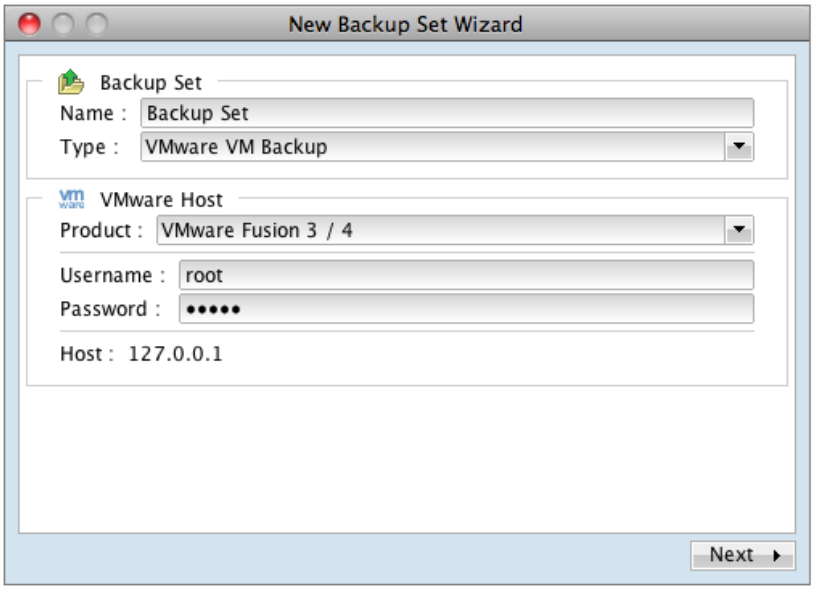
1. Login to the backup application's user interface.

2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.



3. Create a VMware VM Backup set by selecting [VMware VM Backup] from the backup set type dropdown menu.

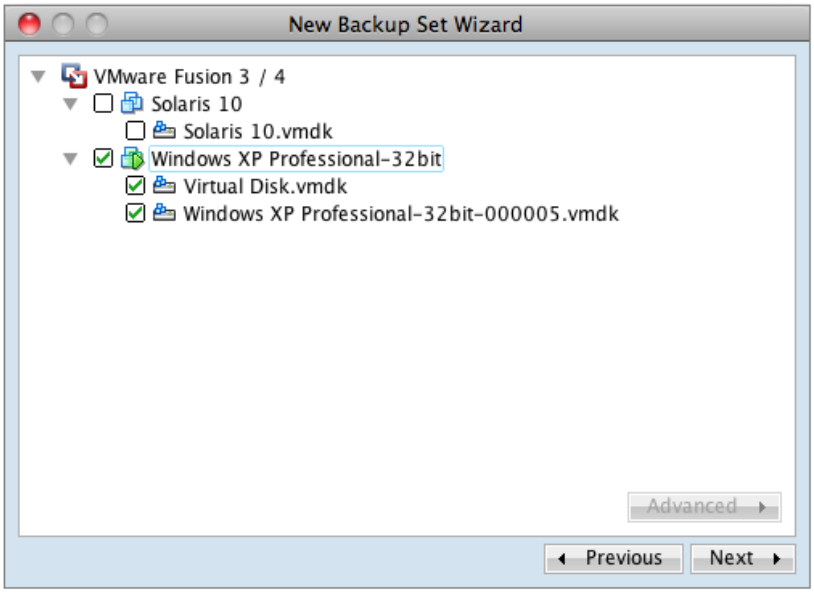
4. Enter the corresponding information required:



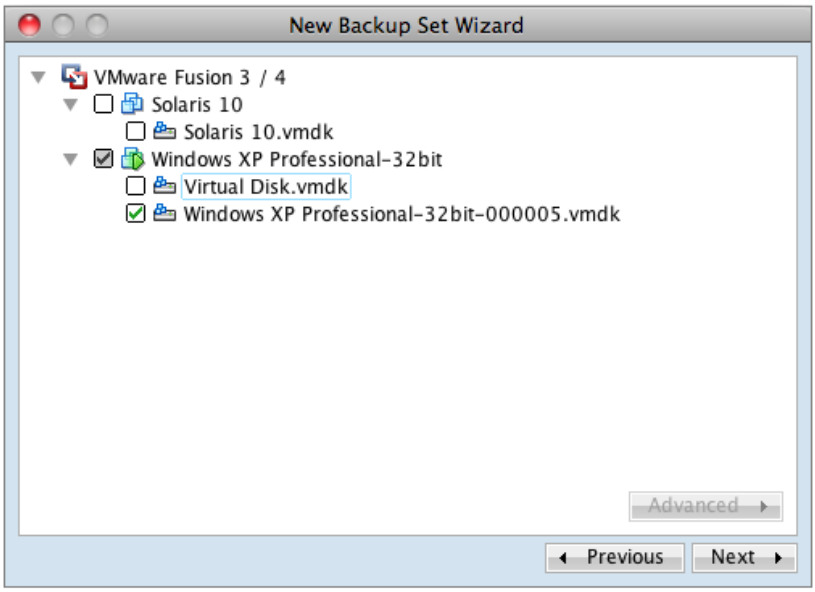
Menu Items	Description
Name	Enter a backup set name of your choice.
Type	Select backup set type [VMware VM Backup].
VMware Host Version	Select host version, for example [VMware Fusion].
Username	Enter the username of the hypervisor administrator.
Password	Enter the password of the hypervisor administrator.
Host	Default to 127.0.0.1, as OBM must be installed on the hypervisor.

5. Select [Next] to proceed.

6. Select the corresponding virtual machines for backup.



7. Alternatively, select individual virtual disk for backup by expanding the corresponding VM sub tree.



Important:
For backup of VM with snapshot, backup of the whole VM is highly recommended (instead of selective virtual disk).

The restoration process for individual virtual disk requires manual editing of VM configuration files.

In-depth knowledge on VMware product is required.

8. Configure a backup schedule for unattended backups.

Note:
Multiple backup schedules of different types can be configured for the same backup set

9. Select an encryption setting for your backup set.
10. Press the [OK] button to complete the configuration of backup set.
11. Scheduled backup will run automatically at the configured schedule time.
12. Click [Backup] button on the left panel to perform a backup immediately.

13.3.6 How to restore virtual machines on VMware Fusion

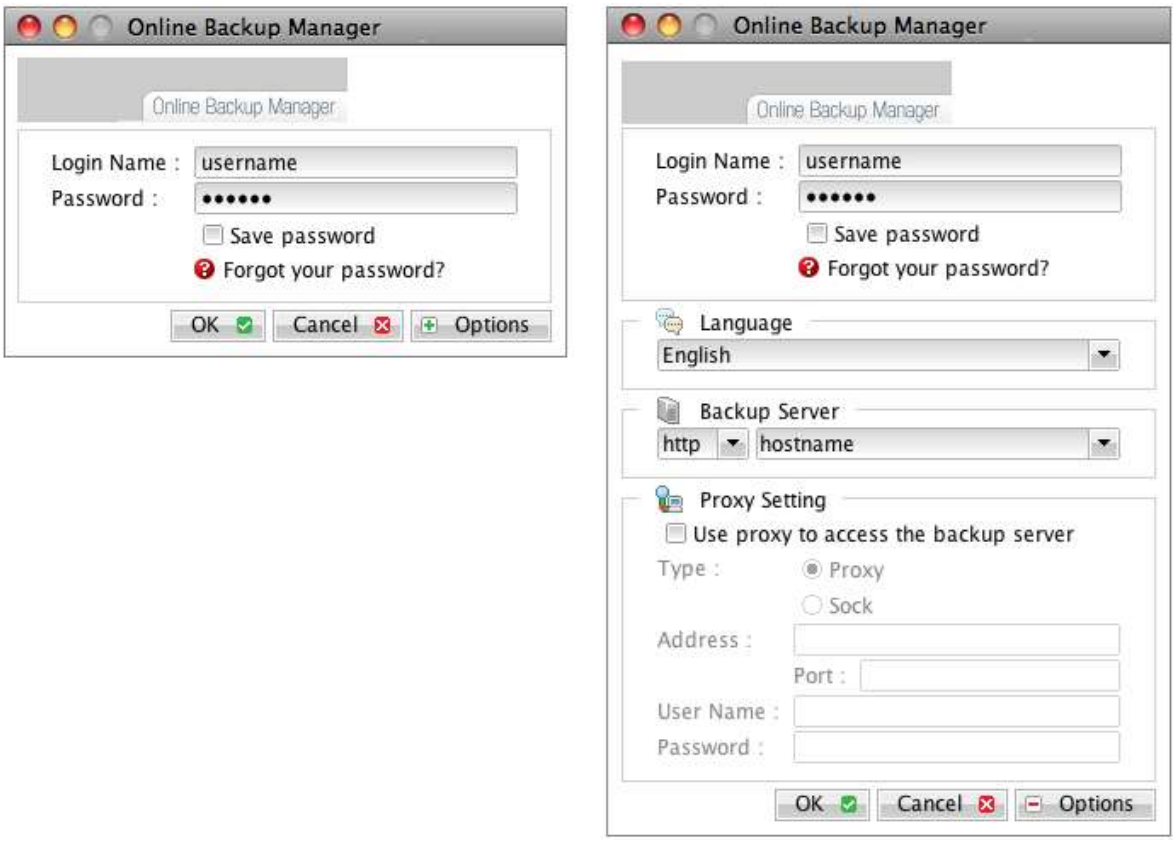
Refer to the following instructions to restore VM running on VMware Fusion.

VM can be restored to the original location with the following condition:

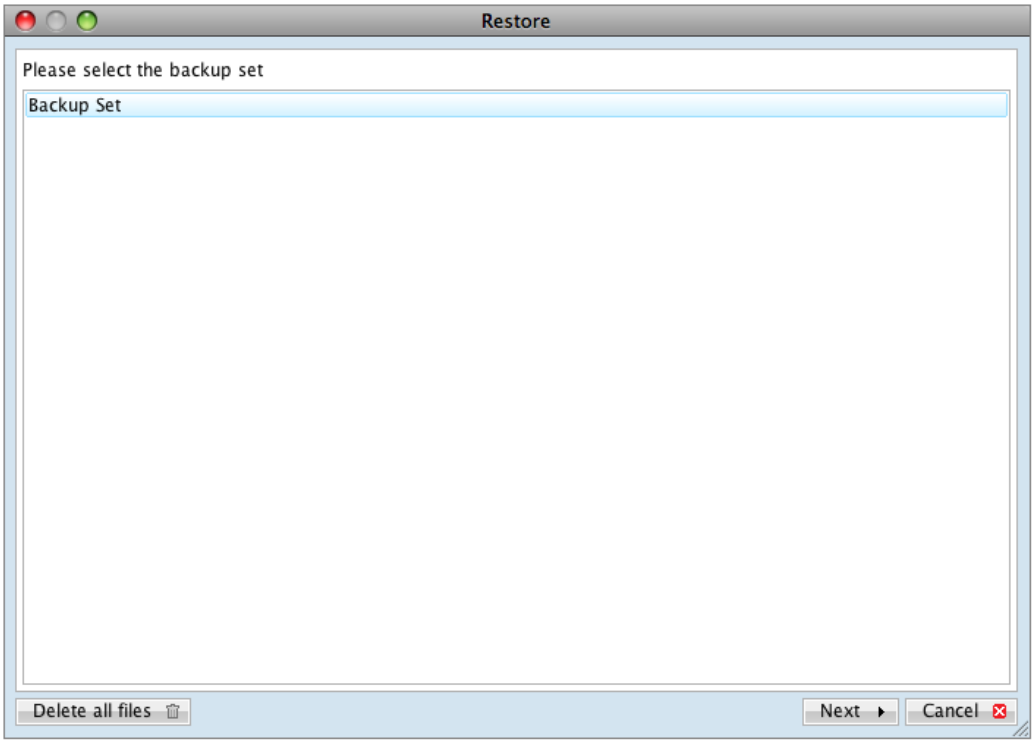
- If the VM to be restored does not exist on the original hypervisor. The VM will be restored as a new virtual machine.
- If the VM to be restored still exist on the original hypervisor. The existing VM will be replaced by the backed up version.

13.3.1.6 How to restore virtual machines to the original hypervisor

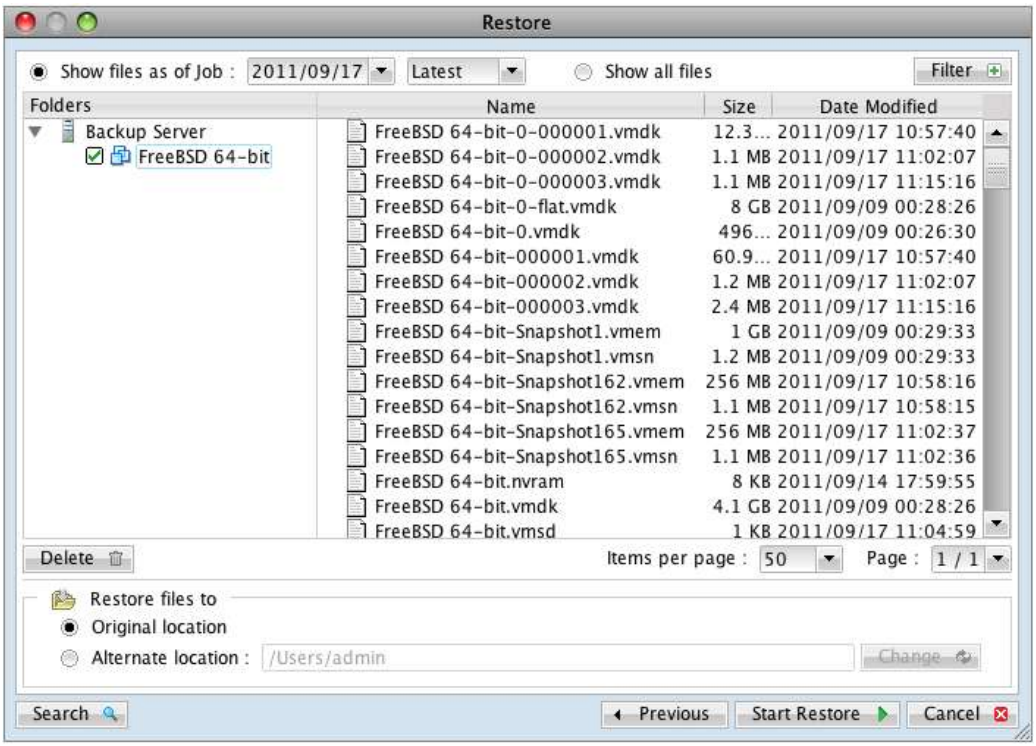
1. Login to the backup application's user interface.



2. Select the [Restore] button and the corresponding backup set.

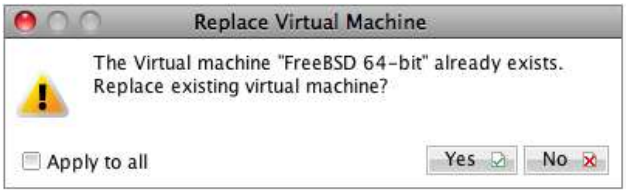


3. Select the virtual machines to be restored and choose [Original Location] for restore files to.



4. Click the [Start Restore] button to begin the restore process.

5. User will be prompted if a virtual machine selected to be restored exist on the hypervisor.



6. When the restore process is completed, the virtual machines will be restored to the original hypervisor.

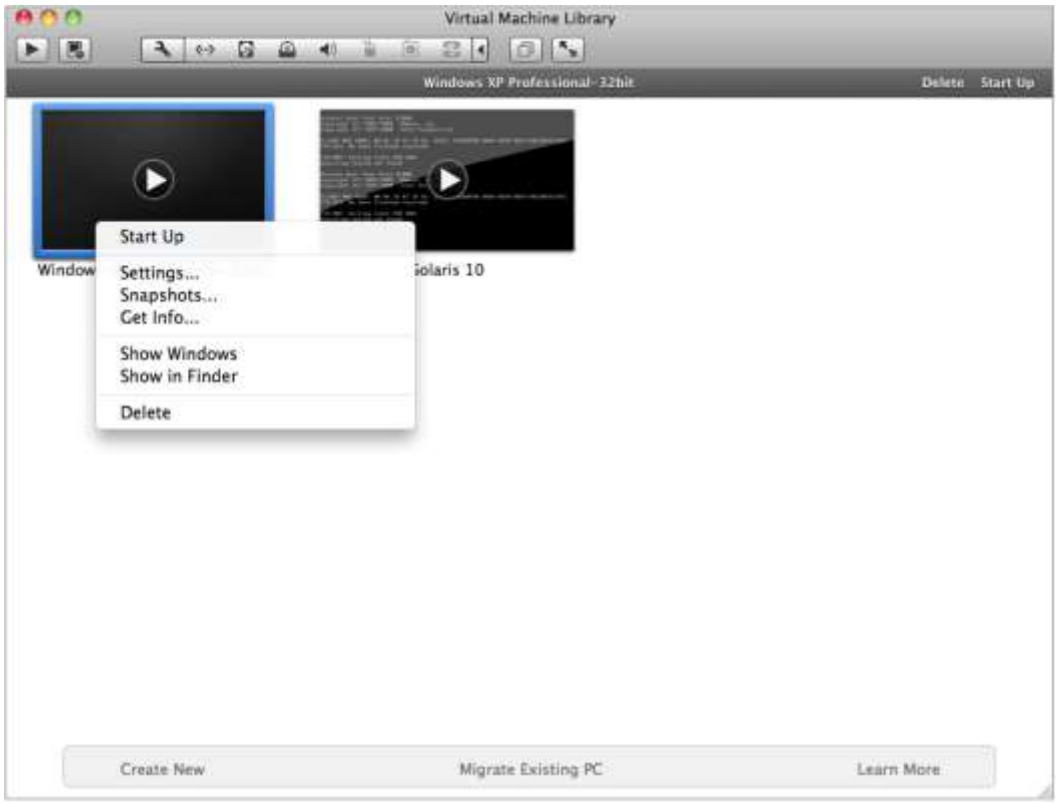
7. For any virtual disk that was not restored (e.g. original backup source did not include all hard disks configured for the VM).

   Continue to the next steps for instruction to remove the missing hard disk from the virtual machine's configuration.

For original virtual machine with no snapshot

1. Open the Virtual Machine Library Window.

2. Control click on the newly restored virtual machine, select [Settings].



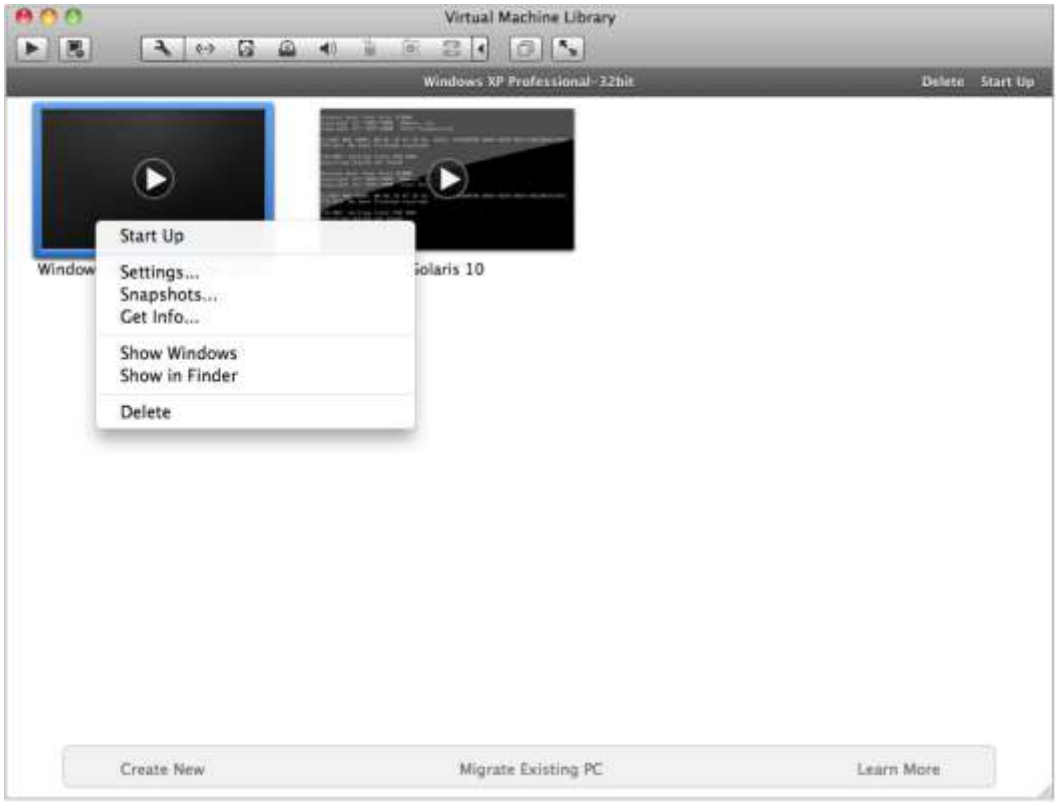
3. Select [Hard Disk].

4. For each virtual disk that was not restored, remove the corresponding hard disk by pressing [Remove Hard Disk].

5. Start the virtual machine afterward.

For original virtual machine with snapshot

1. Open the Virtual Machine Library Window.
2. Control click on the newly restored virtual machine, select [Settings].



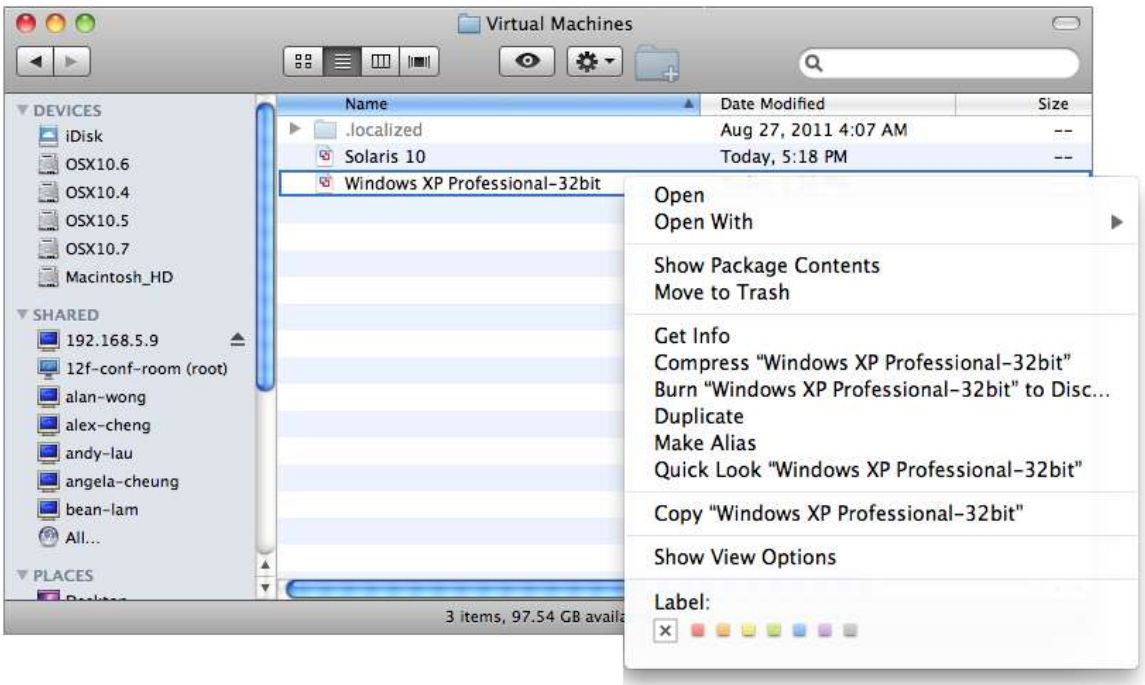
3. Select [Hard Disk].

4. For each virtual disk that was not restored, remove the corresponding hard disk by pressing [Remove Hard Disk].

5. Remove the VM from the Virtual Machine Library Window.

6. Locate the virtual machine's folder location on the hypervisor.

7. Control click on the VM, select [Show Package Contents].



Important:
Serious problem may occur if the configuration files are incorrectly modified; it may prevent the virtual machine from starting.

Please only perform the following procedures if you have in-depth knowledge on VMware product.

8. Delete the lines of the removed virtual disk.

- Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

```
${VM-Location}\${VM-Name}.vmsd
```

- Locate the line of all non existing virtual disk.

Example:

Snapshot 1, SCSI (0:2) Disk 2 is removed.

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
snapshot0.disk2.fileName = "Windows 2008-2.vmdk"
snapshot0.disk2.node = "scsi0:2"
```

- Remove the corresponding lines.

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Perform the same steps for each snapshot.
- Save the changes afterward.

9. Update the number of virtual disk.

- Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

```
${VM-Location}\${VM-Name}.vmsd
```

- Locate the *numDisks* parameter.

Example:

Snapshot 1, if one of the disks is removed, updates the value of *snapshot0.numDisks*

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Modify the line from:

snapshot0.numDisks = "3"

To

snapshot0.numDisks = "2"

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "2"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
```

```
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Perform the same steps for each snapshot.
- Save the changes afterward.

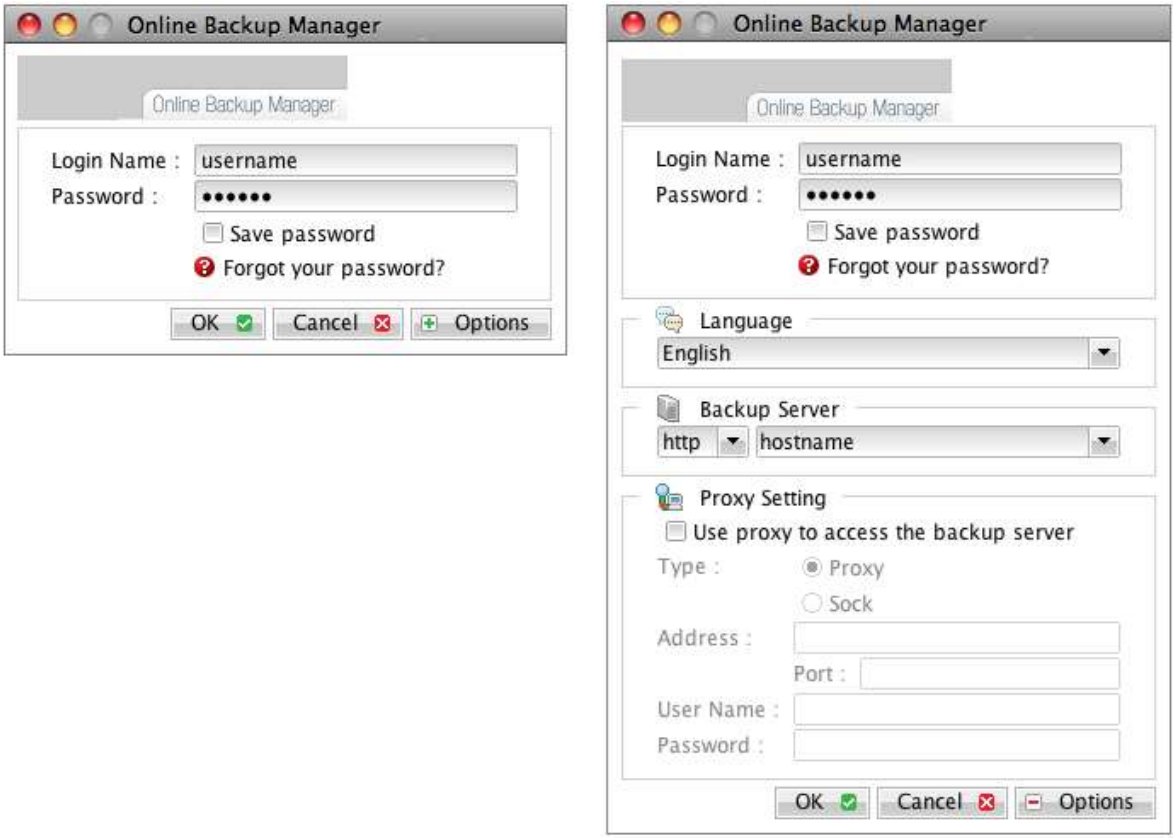
10. Add the VM back into the Virtual Machine Library Window.
11. Remove any existing snapshot.

    Important:
    The restored virtual machine does not support the reversion of previous snapshots if they contain virtual disks not restored.

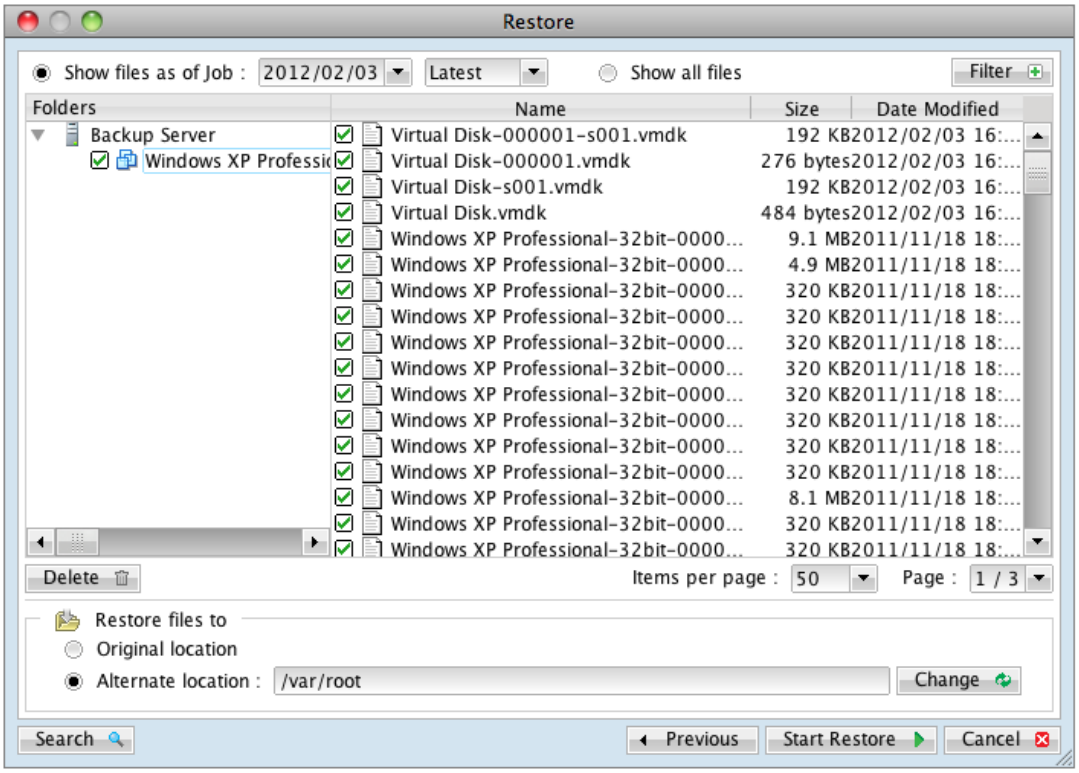
12. Start the virtual machine.

13.3.2.6 How to restore virtual machines to another hypervisor

1. Login to the backup application's user interface.



2. Select the [Restore] button and the corresponding backup set.



3. Select the virtual machines to be restored and choose [Alternate location] for restore files to.

4. Click on the [Change] button and browse to the directory path which you would like to restore the data to.

5. Click the [Start Restore] button to begin the restore process.

6. When the restore process is completed, data of the selected virtual machines will be restored to the specified location.

7. Register the virtual machines on the new hypervisor.

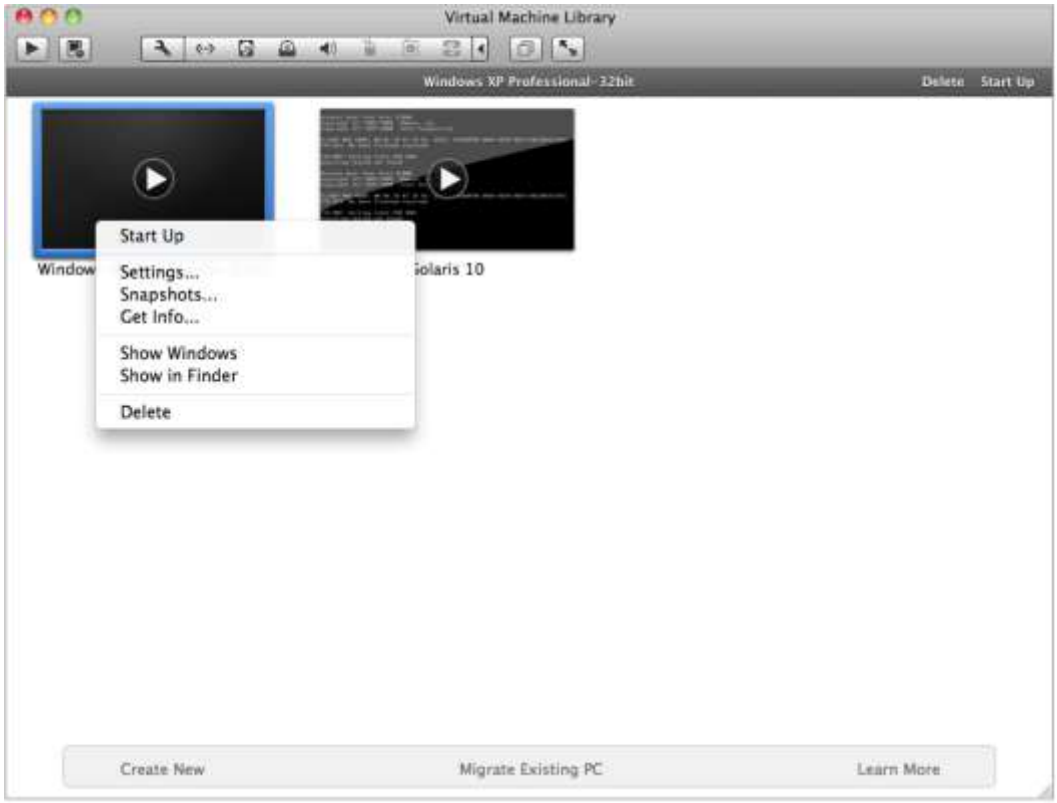
8. For any virtual disk that was not restored (e.g. original backup source did not include all hard disks configured for the VM).

   Continue to the next steps for instruction to remove the missing hard disk from the virtual machine's configuration

For original virtual machine with no snapshot

1. Open the Virtual Machine Library Window.

2. Control click on the newly restored virtual machine, select [Settings].



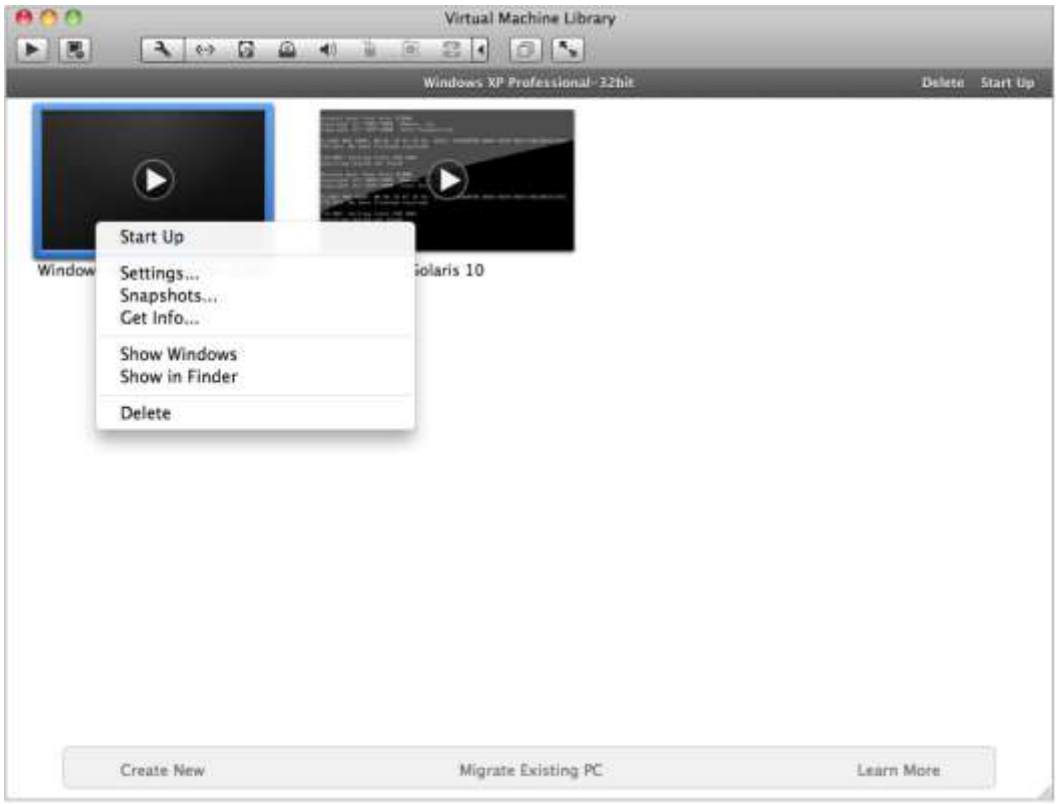
3. Select [Hard Disk].

4. For each virtual disk that was not restored, remove the corresponding hard disk by pressing [Remove Hard Disk].

5. Start the virtual machine afterward.

For original virtual machine with snapshot

1. Open the Virtual Machine Library Window.
2. Right click on the newly restored virtual machine, select [Settings].



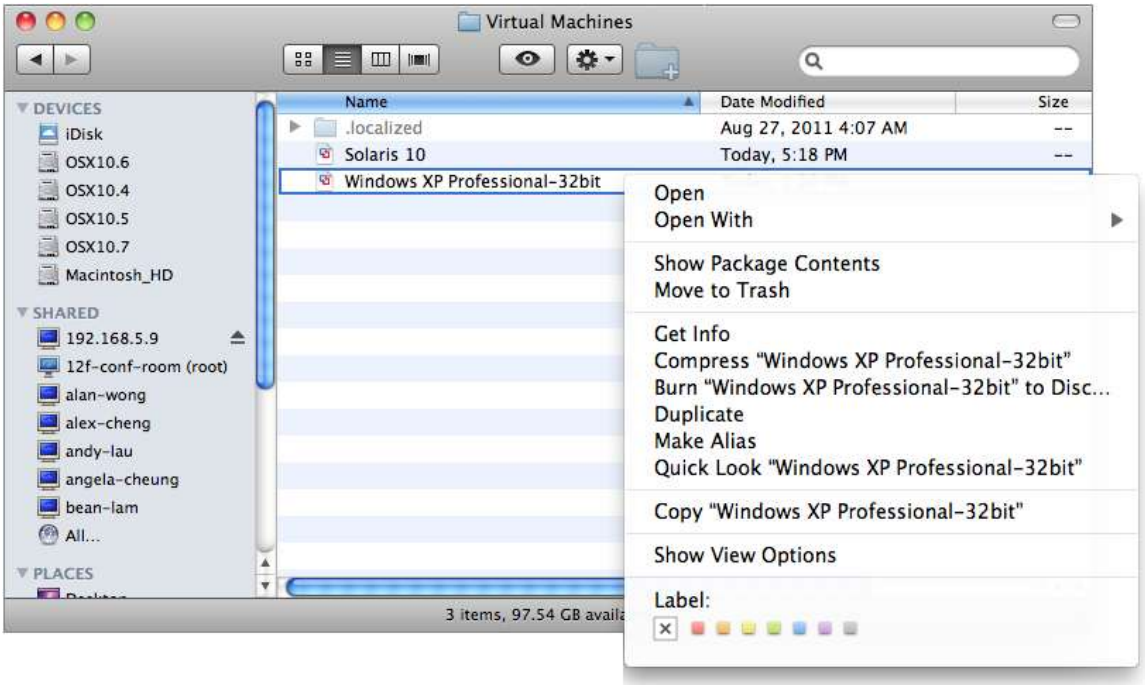
3. Select [Hard Disk].

4. For each virtual disk that was not restored, remove the corresponding hard disk by pressing [Remove Hard Disk].

5. Remove the VM from the Virtual Machine Library Window.

6. Locate the virtual machine's folder location on the hypervisor.

7. Control click on the VM, select [Show Package Contents].



Important:
Serious problem may occur if the configuration files are incorrectly modified; it may prevent the virtual machine from starting.

Please only perform the following procedures if you have in-depth knowledge on VMware product.

8. Delete the lines of the removed virtual disk.

- Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

```
${VM-Location}\${VM-Name}.vmsd
```

- Locate the line of all non existing virtual disk.

Example:

Snapshot 1, SCSI (0:2) Disk 2 is removed.

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
```

```
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
snapshot0.disk2.fileName = "Windows 2008-2.vmdk"
snapshot0.disk2.node = "scsi0:2"
```

- Remove the corresponding lines.

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Perform the same steps for each snapshot.
- Save the changes afterward.

9. Update the number of virtual disk.

- Open the corresponding *${VM-Name}.vmsd* file at the following location with a text editor.

```
${VM-Location}\${VM-Name}.vmsd
```

- Locate the *numDisks* parameter.

Example:

Snapshot 1, if one of the disks is removed, updates the value of *snapshot0.numDisks*

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
```

```
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "3"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Modify the line from:

snapshot0.numDisks = "3"

To

snapshot0.numDisks = "2"

```
snapshot.lastUID = "1"
snapshot.numSnapshots = "1"
snapshot.current = "1"
snapshot0.uid = "1"
snapshot0.filename = "Windows 2008 Snapshot1.vmsn"
snapshot0.displayName = "Snapshot1"
snapshot0.description = ""
snapshot0.createTimeHigh = "309233"
snapshot0.createTimeLow = "1291281261"
snapshot0.numDisks = "2"
snapshot0.disk0.fileName = "Windows 2008-1.vmdk"
snapshot0.disk0.node = "scsi0:0"
snapshot0.disk1.fileName = "Windows 2008-1.vmdk"
snapshot0.disk1.node = "scsi0:1"
```

- Perform the same steps for each snapshot.
- Save the changes afterward.

10. Add the VM back into the Virtual Machine Library Window.
11. Remove any existing snapshot.

    Important:
    The restored virtual machine does not support the reversion of previous snapshots if they contain virtual disks not restored.

12. Start the virtual machine.

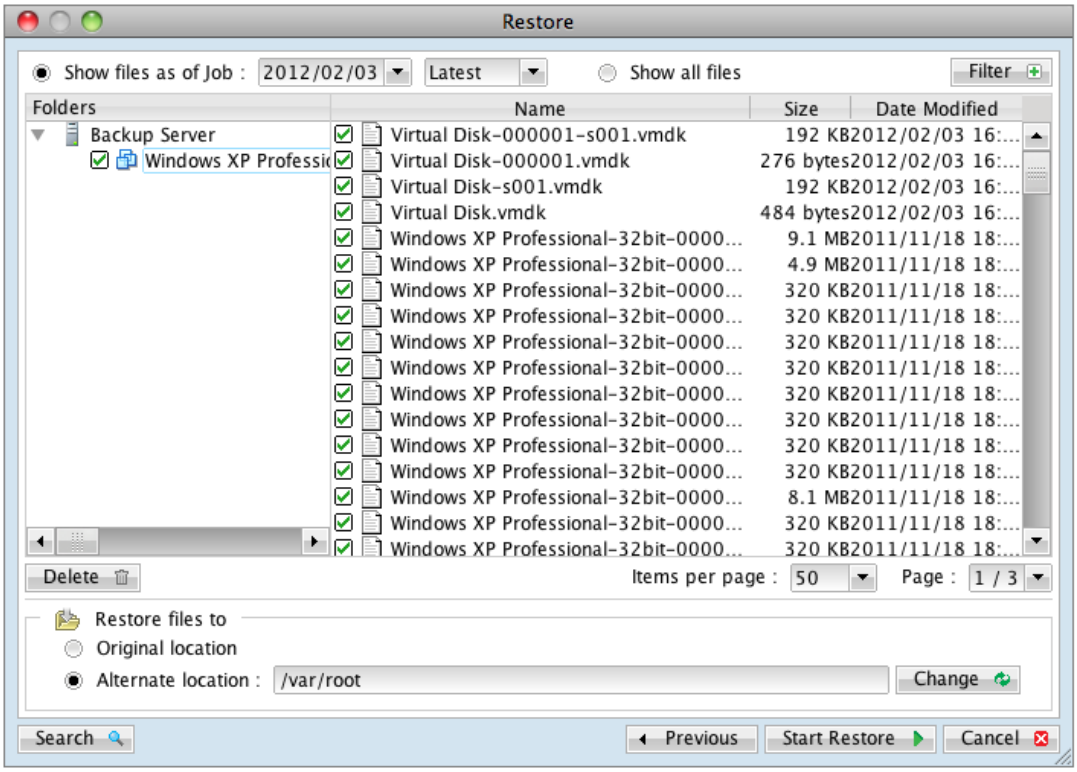
13.3.7 How to restore individual virtual disk

Individual virtual disk can be restored to the original VM, or to be added to a new VM.

13.3.1.7 How to restore individual virtual disk to the original VM

The procedure to restore individual virtual disk to the original VM is very similar to the procedure to restore virtual machine to a new hypervisor.

The main different is that user must select the restore to [Alternate location] option, and select the directory path to the original VM location.

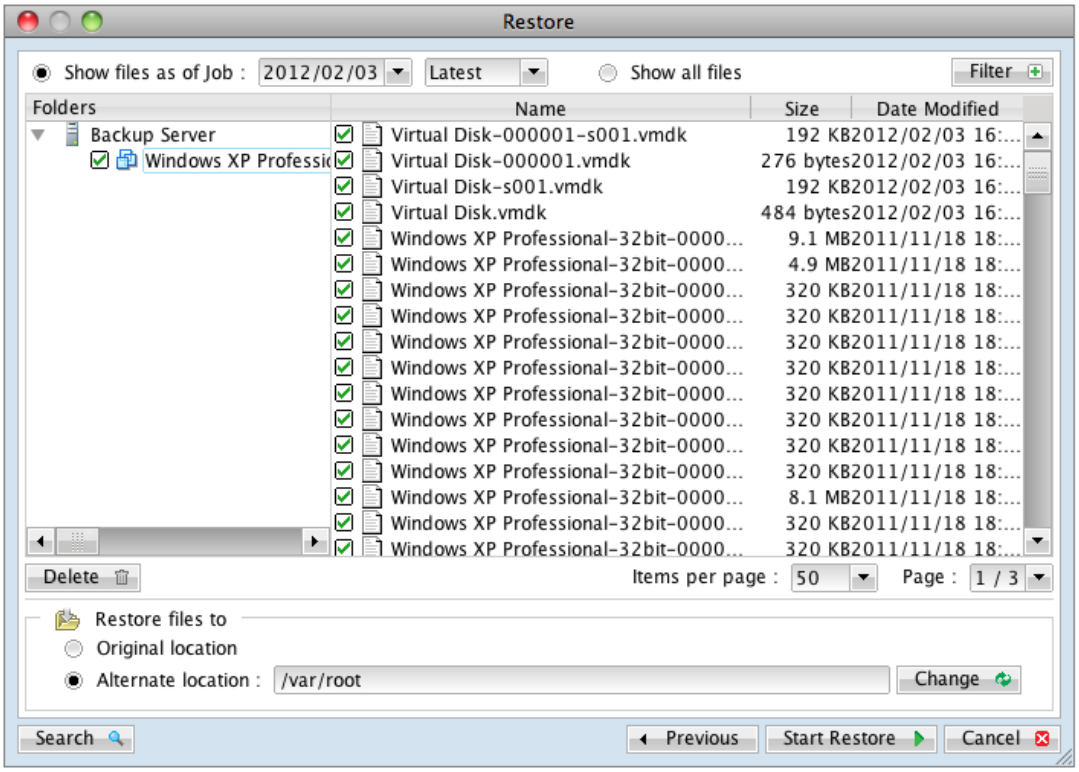


For full instructions, please refer to the above sections.

13.3.2.7 How to restore individual virtual disk to a different VM

1. Login to the backup application's user interface.

2. Select the [Restore] button and the corresponding backup set.


Restore
Show files as of Job : 2012/02/03
Latest
Show all files
Filter
Folders
Name
Size
Date Modified
Backup Server
Windows XP Professi
Virtual Disk-000001-s001.vmdk 192 KB 2012/02/03 16:...
Virtual Disk-000001.vmdk 276 bytes 2012/02/03 16:...
Virtual Disk-s001.vmdk 192 KB 2012/02/03 16:...
Virtual Disk.vmdk 484 bytes 2012/02/03 16:...
Windows XP Professional-32bit-0000... 9.1 MB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 4.9 MB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 8.1 MB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Windows XP Professional-32bit-0000... 320 KB 2011/11/18 18:...
Delete
Items per page : 50
Page : 1 / 3
Restore files to
Original location
Alternate location : /var/root
Change
Search
Previous
Start Restore
Cancel

3. Select the virtual machines to be restored and choose [Alternate location] for restore files to.

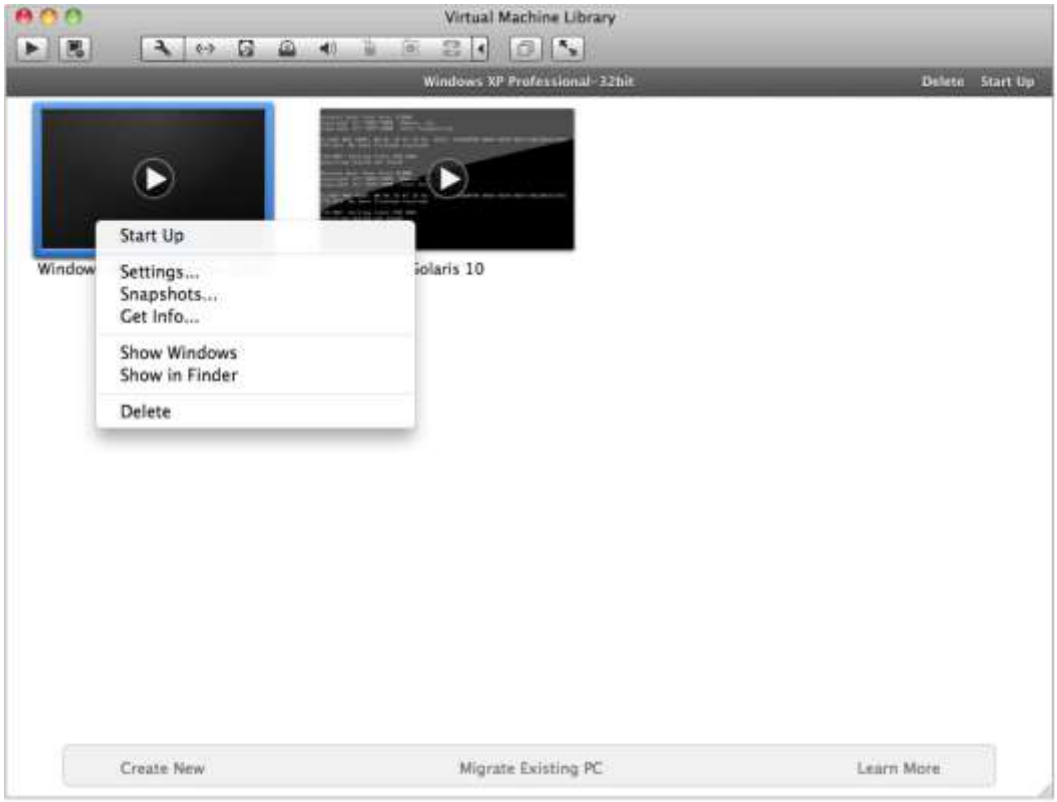
4. Click on the [Change] button and browse to the directory path which you would like to restore the data to.

5. Click the [Start Restore] button to begin the restore process.

6. Open the Virtual Machine Library Window.

7. Powers down the corresponding virtual machine to be restored to.

8. Right click on the corresponding VM, and select [Settings].



9. Select [Add Device] to add the newly restored virtual disk.

10. Select [Existing Hard Disk].

11. In the Open dialog, navigate to the location of the newly restored hard disk file.

12. Select the method for adding the virtual hard disk file.

13. Click [Open] and [Apply].

14. Start the virtual machine.

13.4 VMware Player and Workstation

13.4.1 Supported versions

The VMware VM backup module is supported for the following VMware Player and Workstation versions:

- VMware Player 3.0
- VMware Player 4.0

- VMware Workstation 6.0
- VMware Workstation 6.5
- VMware Workstation 7.0
- VMware Workstation 8.0

For more details, please refer to Help Centre Article:
https://help..com/openArticle.aspx?aid=2323

13.4.2 Backup and restore of virtual machines on VMware Player and Workstation

Backup and restore procedures for VM running on VMware Player and Workstation are very similar to that of VM running on VMware Server.

Please refer to the VMware Server section of this guide for more details.

13.5 Independent disk for VMware virtual machine

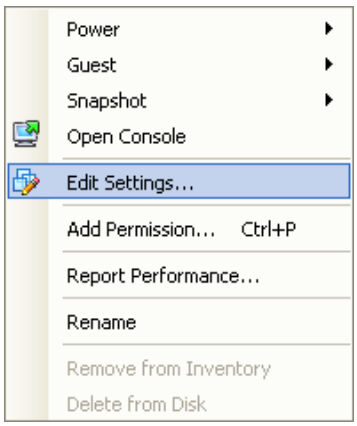
Online (active) backup cannot be performed on virtual machines with Independent Disk. A snapshot cannot be created for an Independent Disk.

If a VM with Independent Disk is online during backup, OBM will skip the backup of any Independent Disk.

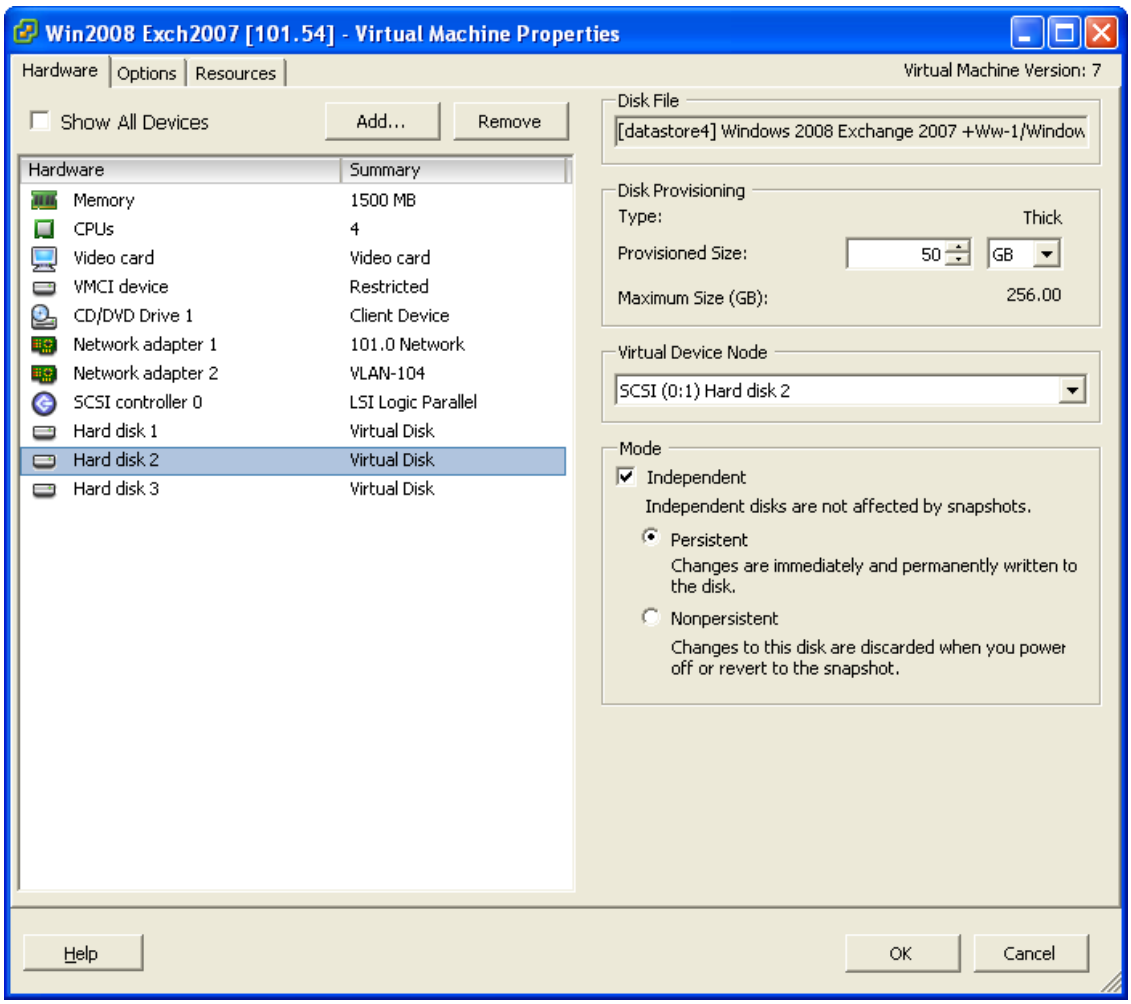
When the virtual machine is restored to original hypervisor, Independent Disk that was not backed up will be missing. To allow the VM to be powered on, please remove the missing disk from the restored VM.

1. Open VMware vSphere Client.

2. Under inventory, right click on the newly restored virtual machine, select [Edit Settings].



3. For each Independent Disk that was not restored, remove the corresponding [Hard disk] from [Hardware].



In some cases, the corresponding VM may not work properly because of the missing disk.

14 Backup / Restore Microsoft Virtual Machines

This chapter describes in detail how to backup and restore virtual machine running on Microsoft Hyper-V Server with OBM.

14.1 Backup virtual machines running on Hyper-V Server (non-cluster environment)

14.1.1 Requirements and recommendations

Please ensure that the following requirements are met by the Hyper-V server:

1. OBM version 6.7 or above is installed on the Hyper-V server.
2. The Hyper-V management tools are installed on the Hyper-V server.
3. Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation.
4. It is recommended that the temporary directory have disk space of at least 50% of the largest sized virtual machine to be backed up.
5. For backup of virtual machine with snapshot, backup of the whole VM instead of individual disk is highly recommended.

14.1.2 Limitations

The following are limitations of the MS VM backup module:

1. Virtual machine backed up with the MS VM backup module can only be restored to the original Hyper-V server.
2. Backup of virtual machine with pass through disk (directly attached physical disk) is not supported.
3. For virtual machine with snapshot, the restoration process for individual virtual disk requires manual editing of VM configuration files.

   In-depth knowledge on Hyper-V is required.
4. The virtual machine cannot start up if the guest operating system virtual disk is not restored.
5. Restore of individual virtual disk to a different virtual machine is only supported for virtual disk with no snapshot.

6. For backup of individual virtual disk, the restored virtual machine does not support the reversion of previous snapshots, if the snapshot contains disks which are not previously backed up by OBM.

14.1.3 Overview

The following steps are performed during a backup job:

1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Commands are issued to the hypervisor to create snapshot (memory dump) of the virtual machine with Volume Shadow Copy.

   Important:
   The corresponding virtual machine will be paused during the snapshot process, and resume when the snapshot is completed.

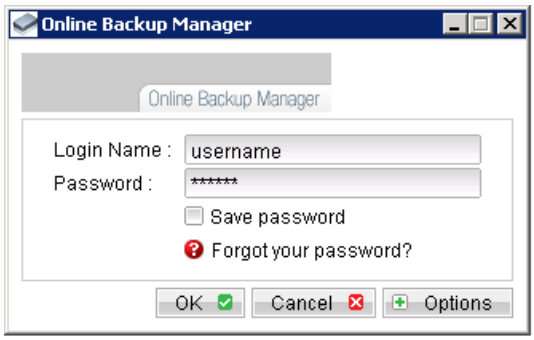
   Do not attempt to start the virtual machine while it is in the saving state. The snapshot created may be invalid.

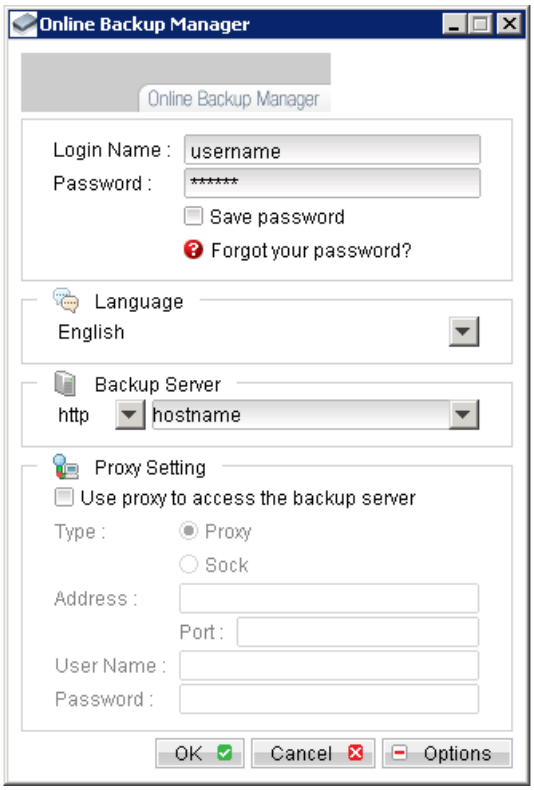
   Furthermore, the corresponding virtual machine uptime will also be reset to 00:00:00 in the Hyper-V Manager.
4. After generating all files, the files are copied to the temporary spool path and upload to OBS.
5. Commands are issued to the hypervisor to remove the Volume Shadow Copy snapshot created.
6. Backup completed successfully.

14.1.4 How to backup Microsoft virtual machines

Refer to the following instructions to backup VM running on Microsoft Hyper-V Server:

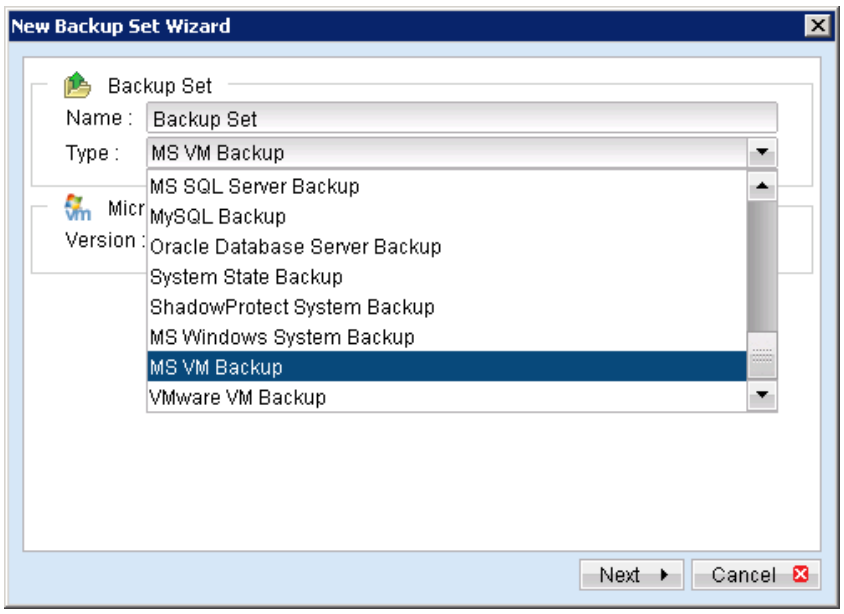
1. Login to the backup application's user interface.



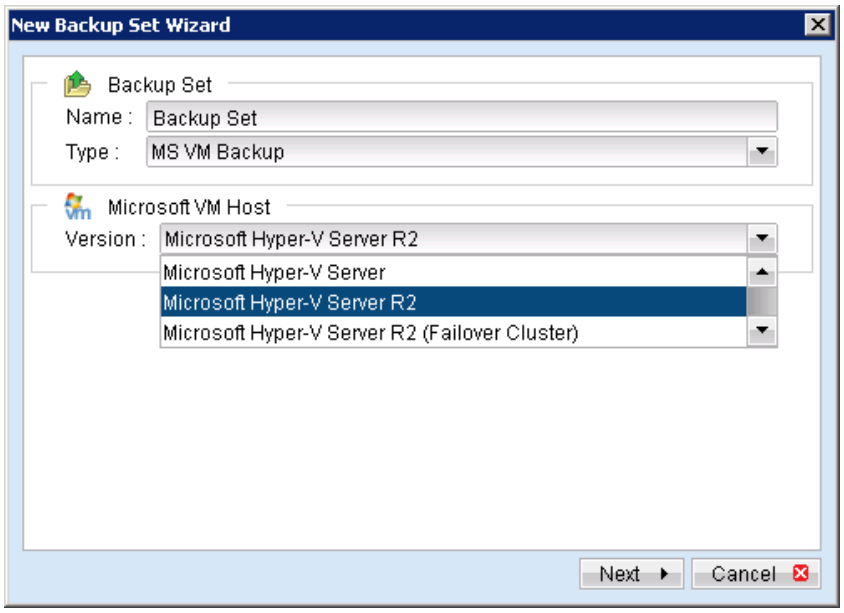


2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

3. Create a MS VM Backup set by selecting [MS VM Backup] from the backup set type dropdown menu.

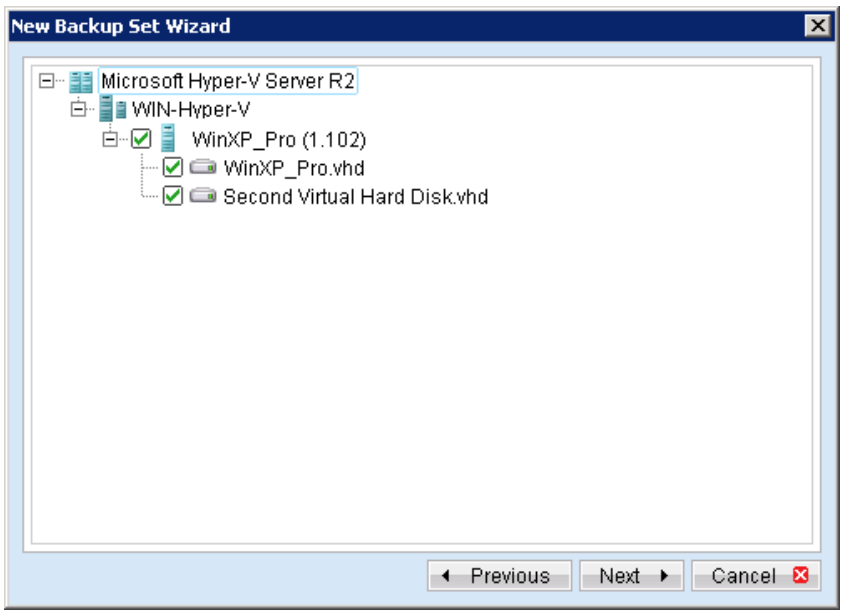


4. Select the version of the hypervisor.

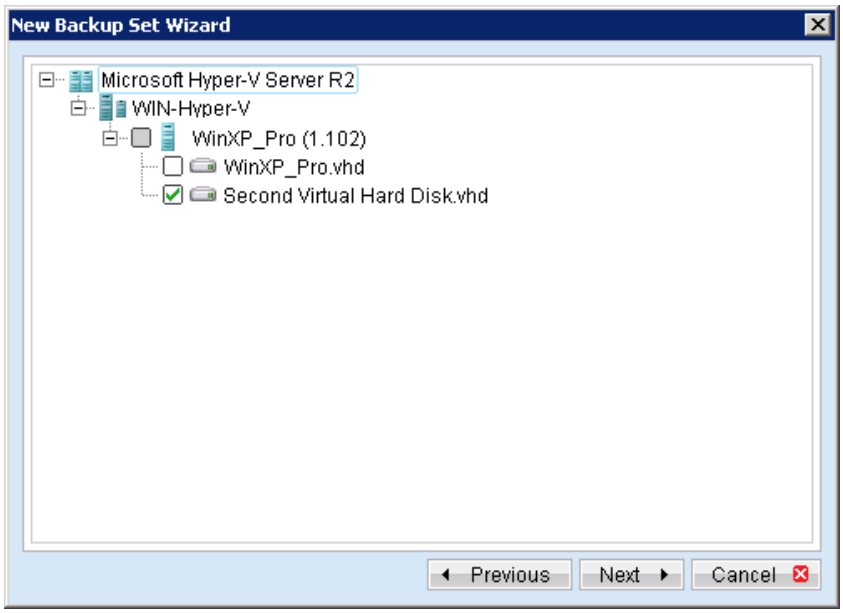


5. Select [Next] to proceed.

6. Select the corresponding virtual machines for backup.



7. Alternatively, select individual virtual disk for backup by expanding the corresponding VM sub tree.



Note:
For backup of individual virtual disk, configuration files of the VM are also backed up.

Important:
For backup of virtual machine with snapshot, backup of the whole VM is highly recommended (instead of selective virtual disk).

8. Configure a backup schedule for unattended backups.

Note:
Multiple backup schedules of different types can be configured for the same backup set.

9. Select an encryption setting for your backup set.
10. Press the [OK] button to complete the configuration of backup set.
11. Scheduled backup will run automatically at the configured schedule time.
12. Click [Backup] button on the left panel to perform a backup immediately.

14.1.5 How to restore Microsoft virtual machines

Refer to the following instructions to restore VM running on Microsoft Hyper-V Server.

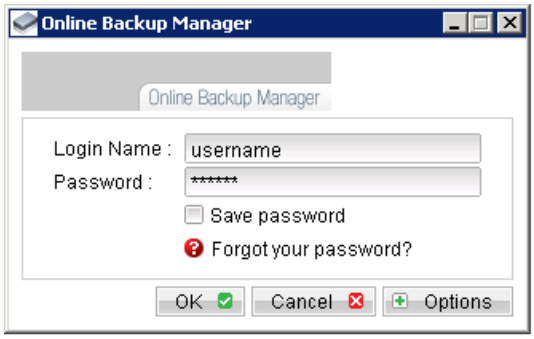
VM can be restored to the original location with the following condition:

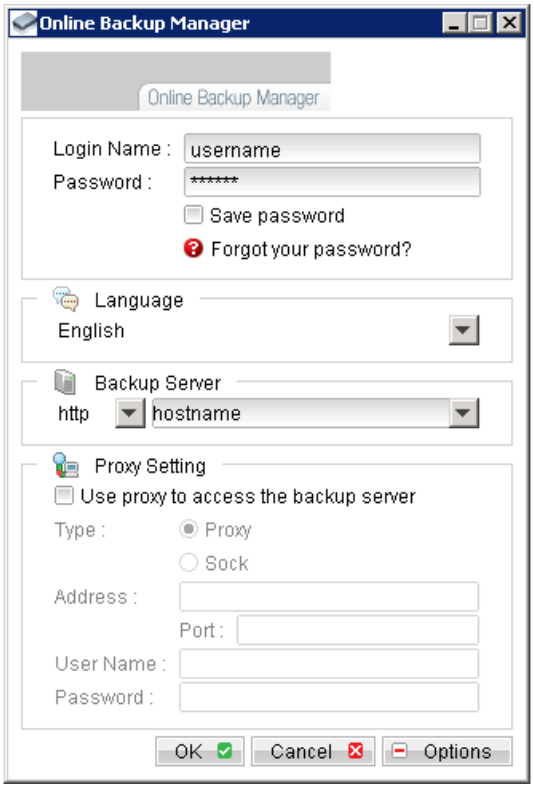
- If the VM to be restored does not exist on the original hypervisor. The VM will be restored as a new virtual machine.

- If the VM to be restored still exist on the original hypervisor. The existing VM will be replaced by the backed up version.

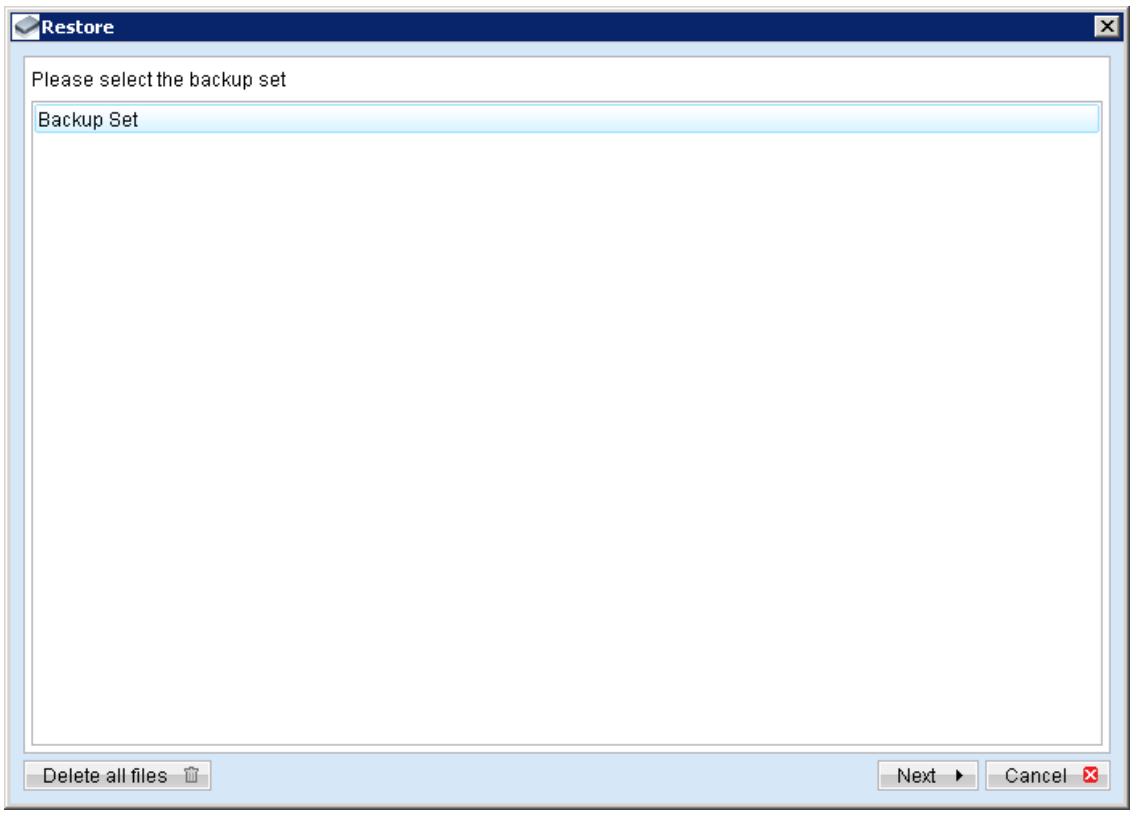
Important:
Virtual machine backed up with the MS VM backup module can only be restored to the original Hyper-V server.

1. Login to the backup application's user interface.

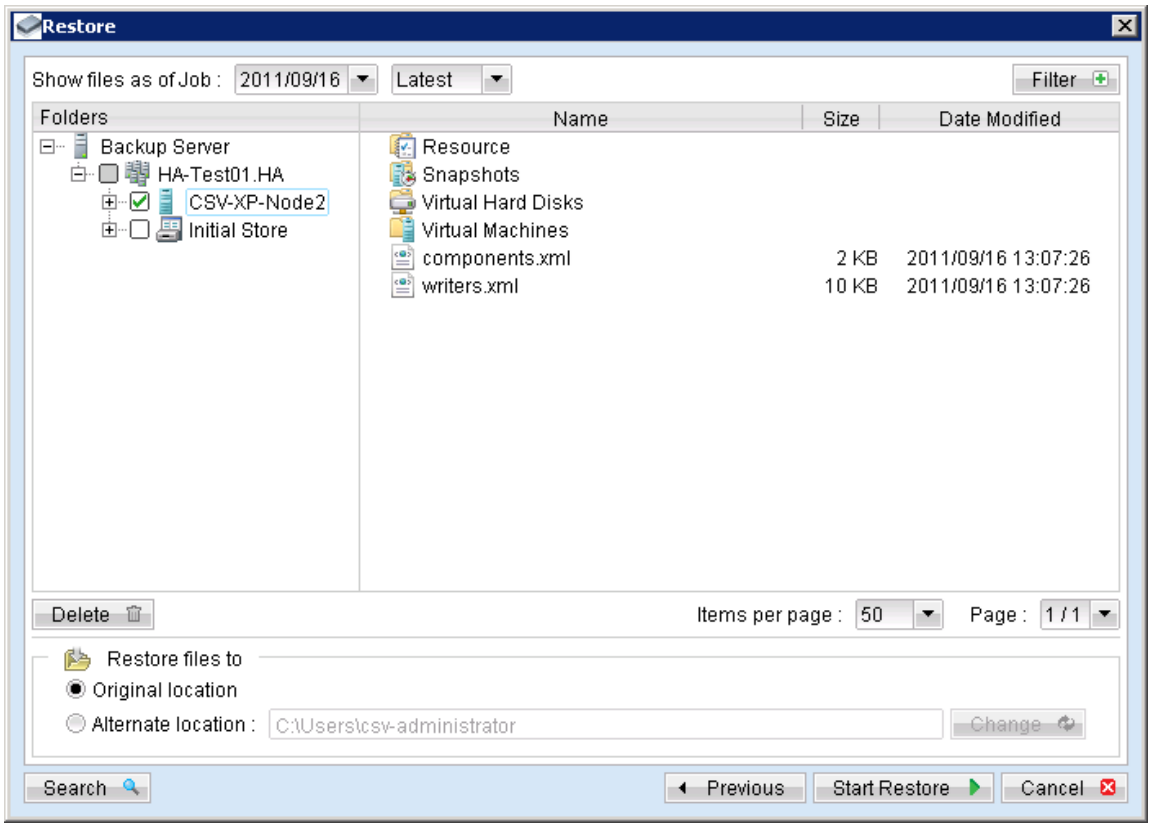




2. Select the [Restore] button and the corresponding backup set.



3. Select the virtual machines to be restored and choose [Original location] for restore files to.

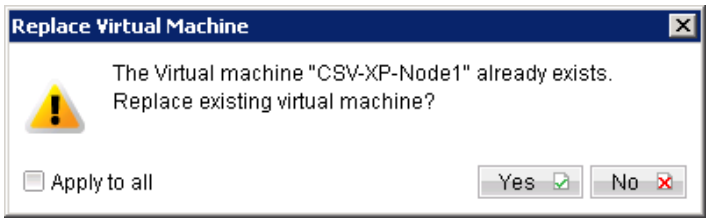


Note:

Select the Initial Store to restore the Authorization Manager Security (role based access control) settings

4. Click the [Start Restore] button to begin the restore process.

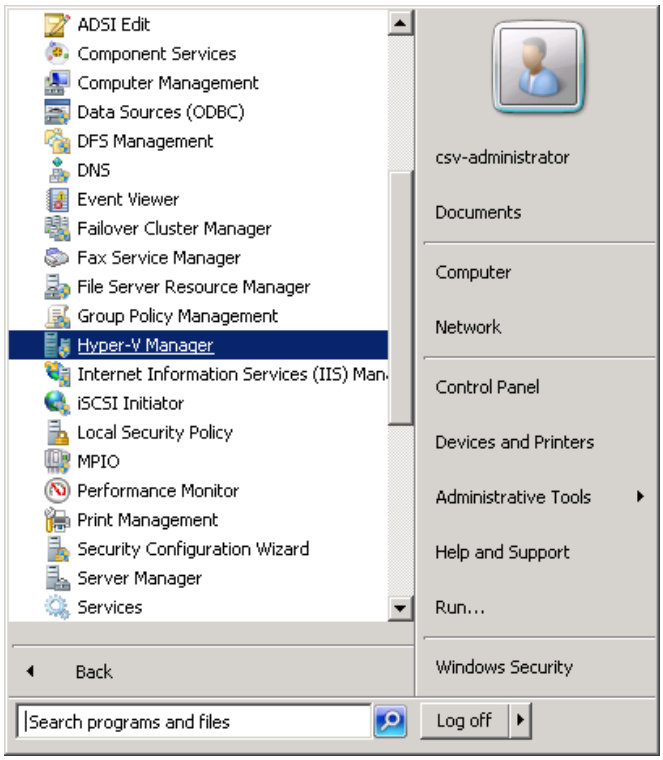
5. User will be prompted if a virtual machine selected to be restored exist on the hypervisor.



Important:
For restore of existing virtual machine (restoring a previous version), the existing virtual machine will be removed before the restore process begin.

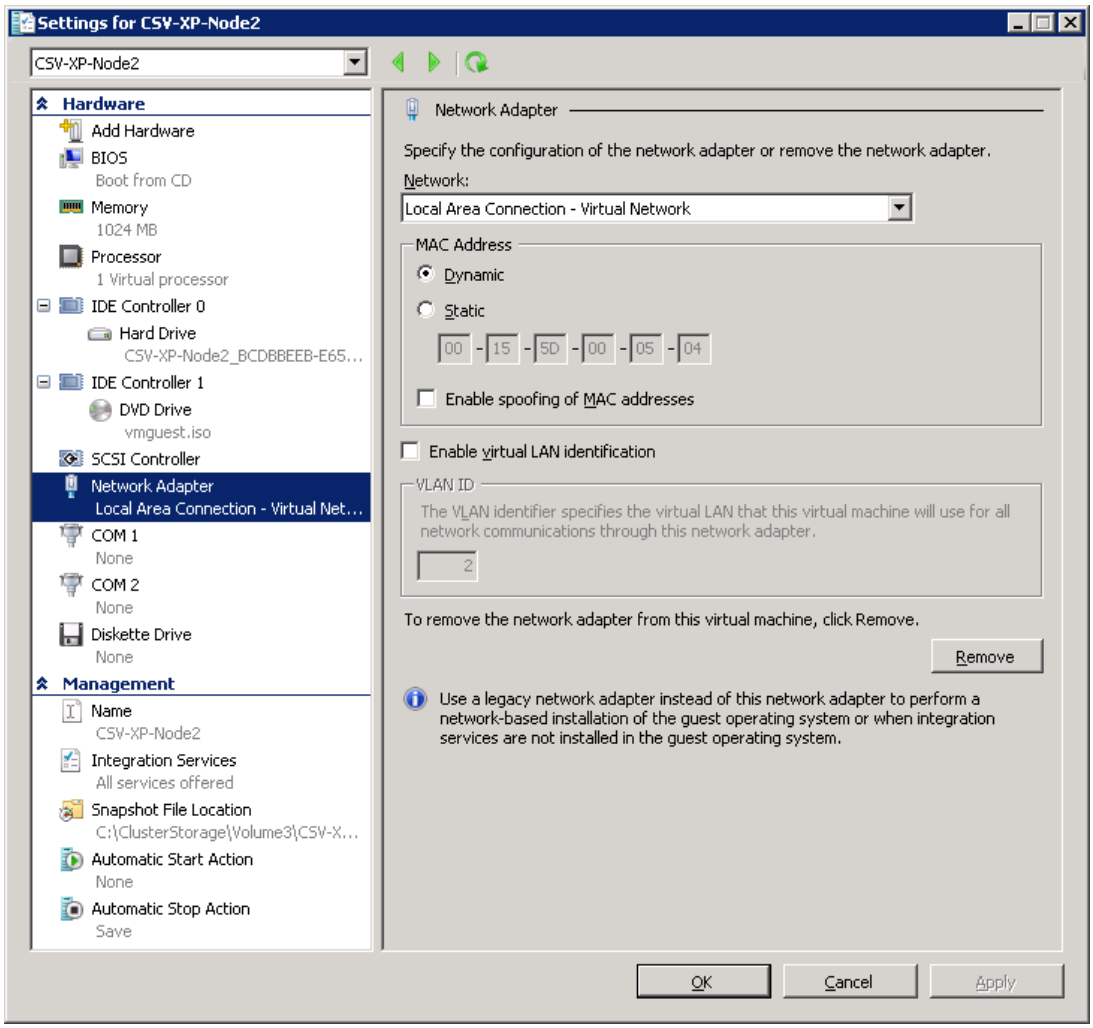
6. When the restore process is completed, the virtual machines will be restored to the original hypervisor.

7. Open Hyper-V Manager, click Start, Administrative Tools and click Hyper-V Manager.



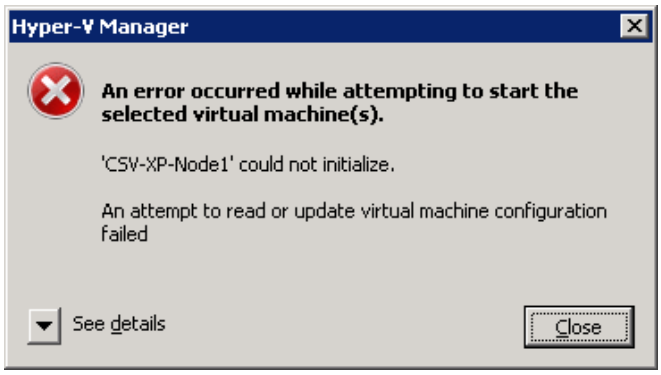
8. Under Virtual Machines, right click on the newly restored virtual machine, select [Setting].

9. Modify settings which may be conflicting with other existing virtual machines (e.g. network setting).



10. Start the virtual machine afterward.

Important:
If the following error is displayed during the startup, please remove the Saved State of the corresponding VM.


Hyper-V Manager
An error occurred while attempting to start the selected virtual machine(s).
'CSV-XP-Node1' could not initialize.
An attempt to read or update virtual machine configuration failed
See details
Close

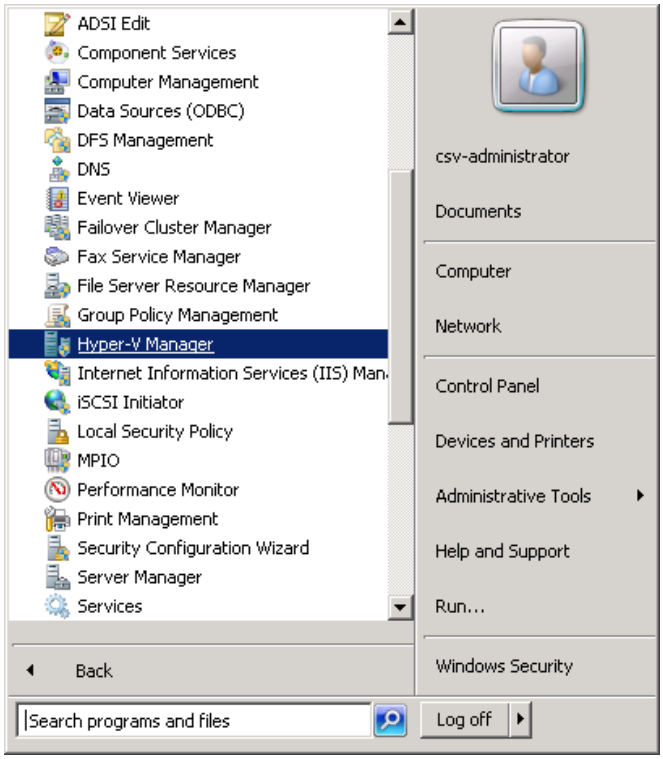
In Hyper-V Manager, right click on the corresponding VM and select [Delete Saved State], start the VM again afterward.

11. For any virtual disk that was not restored (e.g. original backup source did not include all virtual disks configured for the VM).

    Continue to the next steps for instruction to remove the missing virtual disk from the virtual machine's configuration.

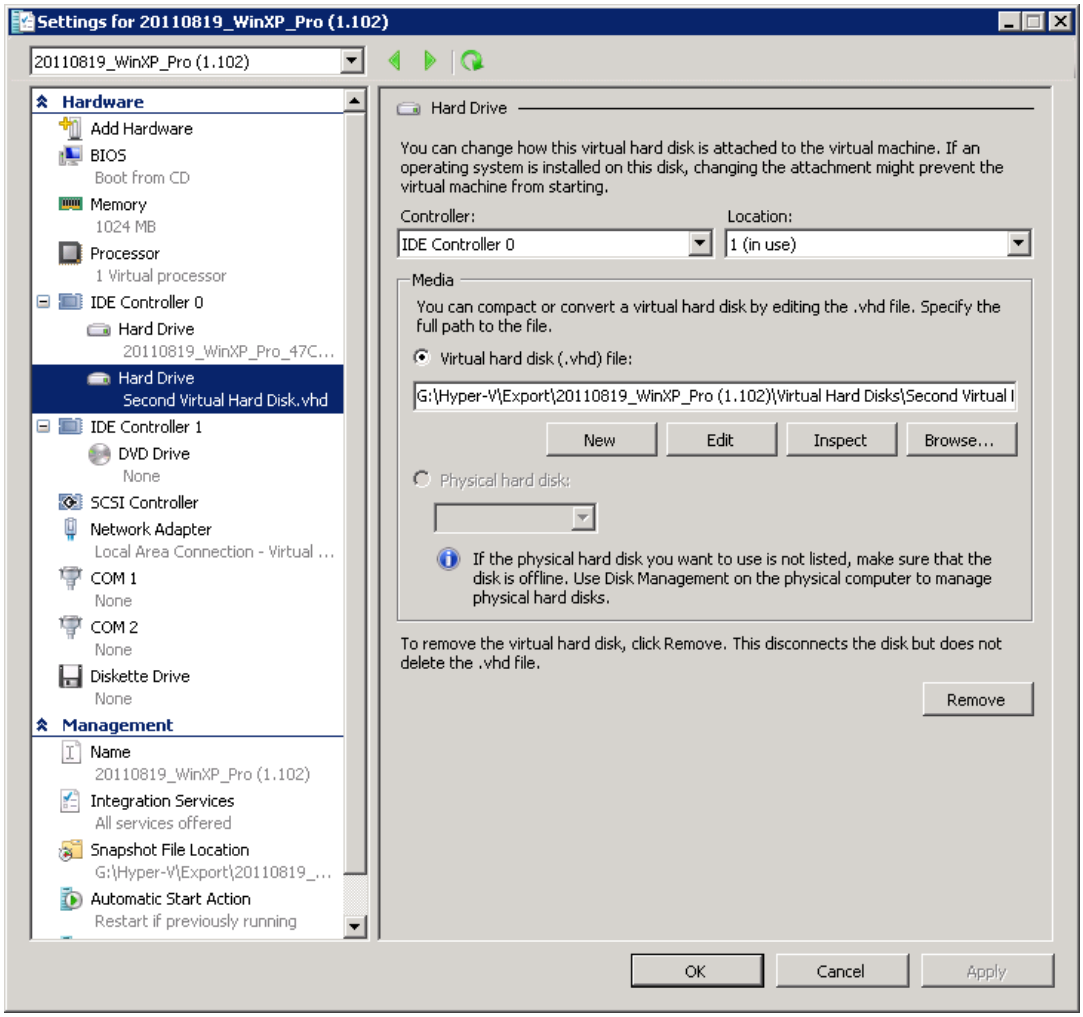
For original virtual machine with no snapshot

1. Open Hyper-V Manager.



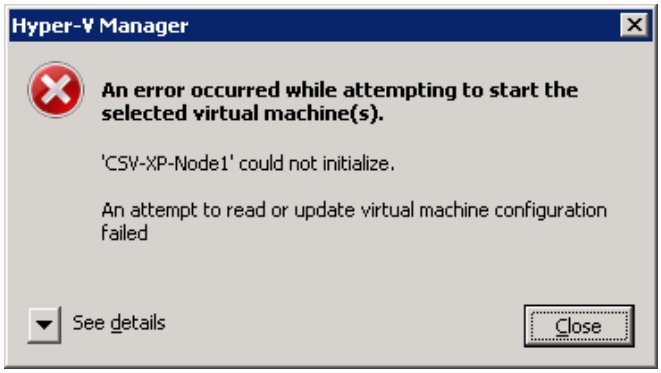
2. Under Virtual Machines, right click on the newly restored virtual machine, select [Setting].

3. For each virtual disk that was not restored, remove the corresponding [Hard Drive] setting from [Hardware].



4. Start the virtual machine afterward.

Important:
If the following error is displayed during the startup, please remove the Saved State of the corresponding VM.


Hyper-V Manager
An error occurred while attempting to start the selected virtual machine(s).
'CSV-XP-Node1' could not initialize.
An attempt to read or update virtual machine configuration failed
See details
Close

In Hyper-V Manager, right click on the corresponding VM and select [Delete Saved State], start the VM again afterward.

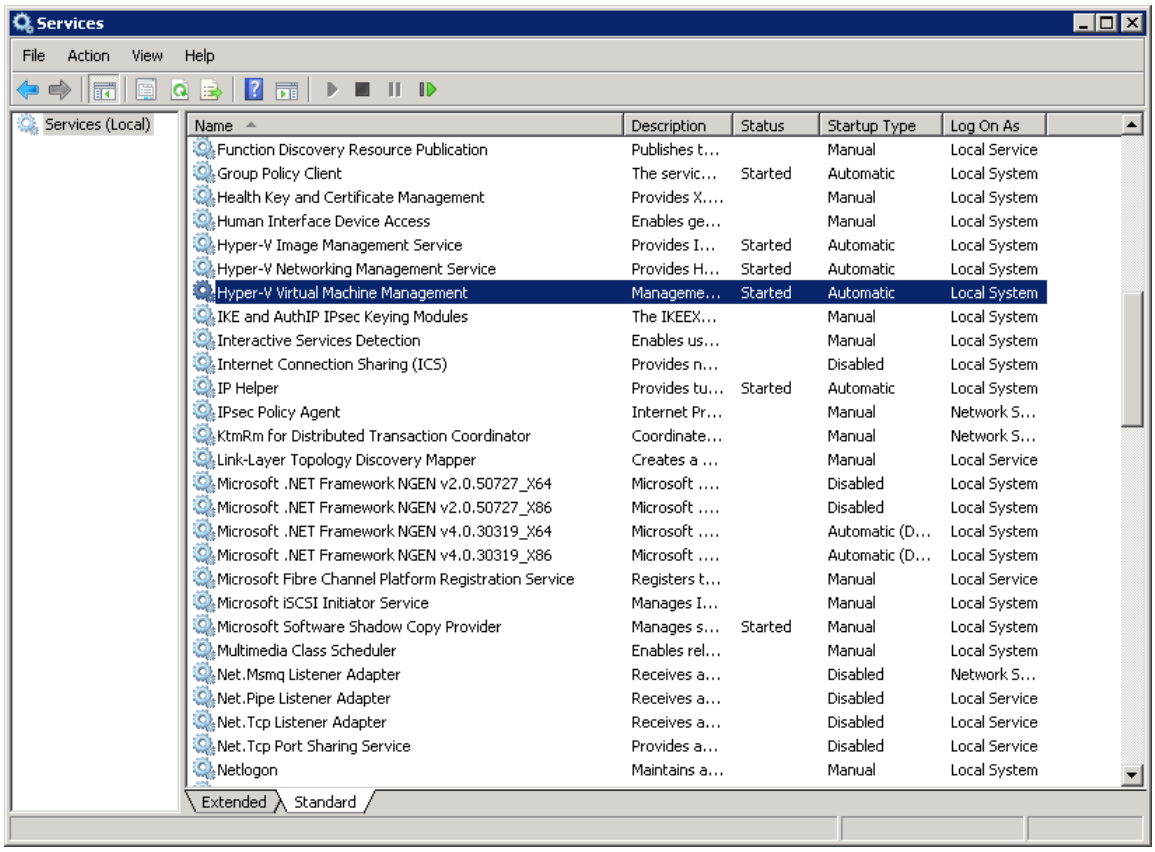
For original virtual machine with snapshot

1. Locate the virtual machine's folder location on the Hyper-V server.

   Important:
   Serious problem may occur if the configuration files are incorrectly modified; it may prevent the virtual machine from starting.

   Please only perform the following procedures if you have in-depth knowledge on Hyper-V management.

2. Stop the Hyper-V Virtual Machine Management service.


Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
Function Discovery Resource Publication Publishes t... Manual Local Service
Group Policy Client The servic... Started Automatic Local System
Health Key and Certificate Management Provides X.... Manual Local System
Human Interface Device Access Enables ge... Manual Local System
Hyper-V Image Management Service Provides I... Started Automatic Local System
Hyper-V Networking Management Service Provides H... Started Automatic Local System
Hyper-V Virtual Machine Management Manageme... Started Automatic Local System
IKE and AuthIP IPsec Keying Modules The IKEEX... Manual Local System
Interactive Services Detection Enables us... Manual Local System
Internet Connection Sharing (ICS) Provides n... Disabled Local System
IP Helper Provides tu... Started Automatic Local System
IPsec Policy Agent Internet Pr... Manual Network S...
KtmRm for Distributed Transaction Coordinator Coordinate... Manual Network S...
Link-Layer Topology Discovery Mapper Creates a ... Manual Local Service
Microsoft .NET Framework NGEN v2.0.50727_X64 Microsoft .... Disabled Local System
Microsoft .NET Framework NGEN v2.0.50727_X86 Microsoft .... Disabled Local System
Microsoft .NET Framework NGEN v4.0.30319_X64 Microsoft .... Automatic (D... Local System
Microsoft .NET Framework NGEN v4.0.30319_X86 Microsoft .... Automatic (D... Local System
Microsoft Fibre Channel Platform Registration Service Registers t... Manual Local Service
Microsoft iSCSI Initiator Service Manages I... Manual Local System
Microsoft Software Shadow Copy Provider Manages s... Started Manual Local System
Multimedia Class Scheduler Enables rel... Manual Local System
Net.Msmq Listener Adapter Receives a... Disabled Network S...
Net.Pipe Listener Adapter Receives a... Disabled Local Service
Net.Tcp Listener Adapter Receives a... Disabled Local Service
Net.Tcp Port Sharing Service Provides a... Disabled Local Service
Netlogon Maintains a... Manual Local System
Extended Standard

3. Remove the corresponding entry from the Virtual Machine configuration *${VM-GUID}.xml* file.

   - Open the corresponding *${VM-GUID}.xml* file at the following location with a text editor.

```
${VM-Location}\Virtual Machine\${VM-GUID}.xml
```

   - Locate the line of all non existing VHD.

```
<controller0>
    <drive0>
        <pathname type="string">D:\Hyper-V\Virtual Machine
         Name\Virtual Hard Disks\Name_GUID.avhd</pathname>
        <type type="string">VHD</type>
    </drive0>
    <drive1>
        <pathname type="string">D:\Hyper-V\Virtual Machine
         Name\Virtual Hard
         Disks\Second_Disk_GUID.avhd</pathname>
        <type type="string">VHD</type>
    </drive1>
</controller0>
```

   - Modify the line from:

     <type type="string">VHD</type>

     To

     <type type="string">NONE</type>

```
<controller0>
    <drive0>
        <pathname type="string">D:\Hyper-V\Virtual Machine
         Name\Virtual Hard Disks\Name_GUID.avhd</pathname>
        <type type="string">VHD</type>
    </drive0>
    <drive1>
        <pathname type="string">D:\Hyper-V\Virtual Machine
         Name\Virtual Hard
         Disks\Second_Disk_GUID.avhd</pathname>
        <type type="string">NONE</type>
    </drive1>
</controller0>
```

   - Save the changes afterward.

4. Remove the corresponding entry from the Snapshot configuration *${GUID}.xml* file.

   - Open the corresponding snapshot's *${GUID}.xml* file at the following location with a text editor.

```
${VM-Location}\Snapshots\${GUID}.xml
```

   - Locate the line of all non existing virtual disk.

```
<controller0>
    <drive0>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard Disks\Name_GUID.vhd</pathname>
        <type type="string">VHD</type>
    </drive0>
    <drive1>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard
        Disks\Second_Disk_GUID.vhd</pathname>
        <type type="string">VHD</type>
    </drive1>
</controller0>
```

   - Modify the line from:

     <type type="string">VHD</type>

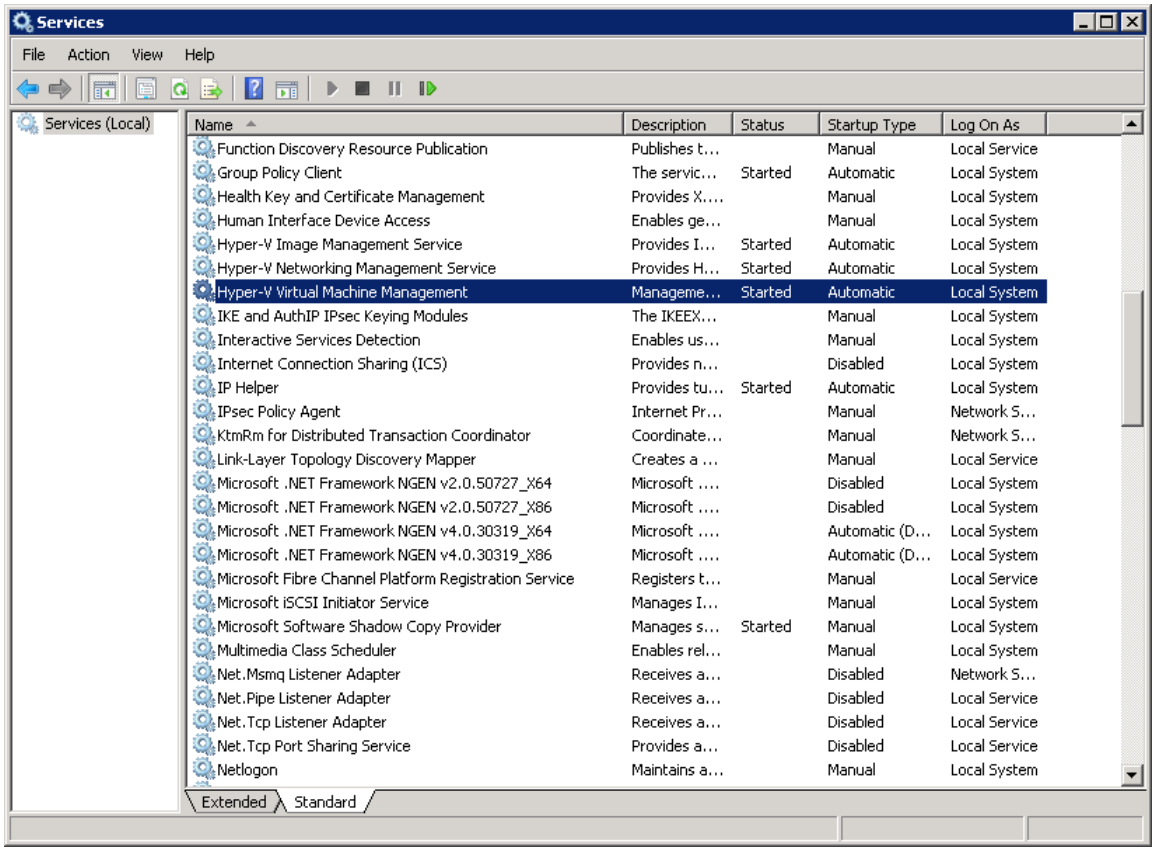
     To

     <type type="string">NONE</type>

```
<controller0>
    <drive0>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard Disks\Name_GUID.vhd</pathname>
        <type type="string">VHD</type>
    </drive0>
    <drive1>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard
        Disks\Second_Disk_GUID.vhd</pathname>
        <type type="string">NONE</type>
    </drive1>
</controller0>
```

- Repeat the same step for each snapshot.

5. Start the Hyper-V Virtual Machine Management service.

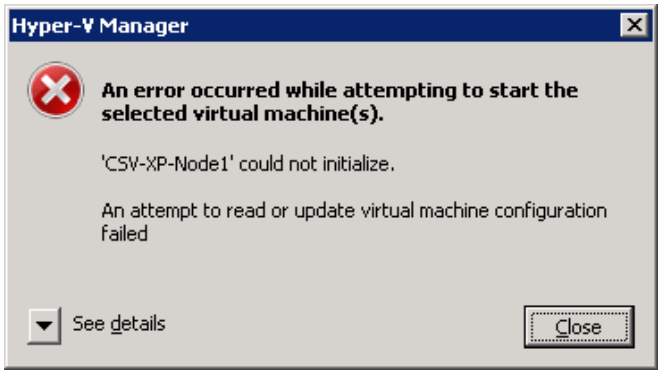

Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
Function Discovery Resource Publication Publishes t... Manual Local Service
Group Policy Client The servic... Started Automatic Local System
Health Key and Certificate Management Provides X.... Manual Local System
Human Interface Device Access Enables ge... Manual Local System
Hyper-V Image Management Service Provides I... Started Automatic Local System
Hyper-V Networking Management Service Provides H... Started Automatic Local System
Hyper-V Virtual Machine Management Manageme... Started Automatic Local System
IKE and AuthIP IPsec Keying Modules The IKEEX... Manual Local System
Interactive Services Detection Enables us... Manual Local System
Internet Connection Sharing (ICS) Provides n... Disabled Local System
IP Helper Provides tu... Started Automatic Local System
IPsec Policy Agent Internet Pr... Manual Network S...
KtmRm for Distributed Transaction Coordinator Coordinate... Manual Network S...
Link-Layer Topology Discovery Mapper Creates a ... Manual Local Service
Microsoft .NET Framework NGEN v2.0.50727_X64 Microsoft .... Disabled Local System
Microsoft .NET Framework NGEN v2.0.50727_X86 Microsoft .... Disabled Local System
Microsoft .NET Framework NGEN v4.0.30319_X64 Microsoft .... Automatic (D... Local System
Microsoft .NET Framework NGEN v4.0.30319_X86 Microsoft .... Automatic (D... Local System
Microsoft Fibre Channel Platform Registration Service Registers t... Manual Local Service
Microsoft iSCSI Initiator Service Manages I... Manual Local System
Microsoft Software Shadow Copy Provider Manages s... Started Manual Local System
Multimedia Class Scheduler Enables rel... Manual Local System
Net.Msmq Listener Adapter Receives a... Disabled Network S...
Net.Pipe Listener Adapter Receives a... Disabled Local Service
Net.Tcp Listener Adapter Receives a... Disabled Local Service
Net.Tcp Port Sharing Service Provides a... Disabled Local Service
Netlogon Maintains a... Manual Local System
Extended Standard

6. Remove any existing snapshot.

Important:
The restored virtual machine does not support the reversion of previous snapshots if they contain virtual disks not restored.

7. Start the virtual machine.

Important:
If the following error is displayed during the startup, please remove the Saved State of the corresponding VM.


Hyper-V Manager
An error occurred while attempting to start the selected virtual machine(s).
'CSV-XP-Node1' could not initialize.
An attempt to read or update virtual machine configuration failed
See details
Close

In Hyper-V Manager, right click on the corresponding VM and select [Delete Saved State], start the VM again afterward.

14.1.6 How to restore individual virtual disk

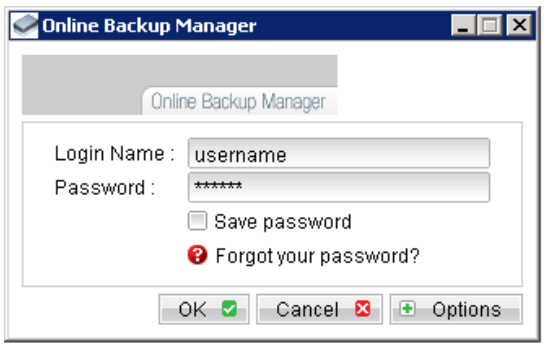
Individual virtual disk can be restored to the original VM, or to be added to a new VM.

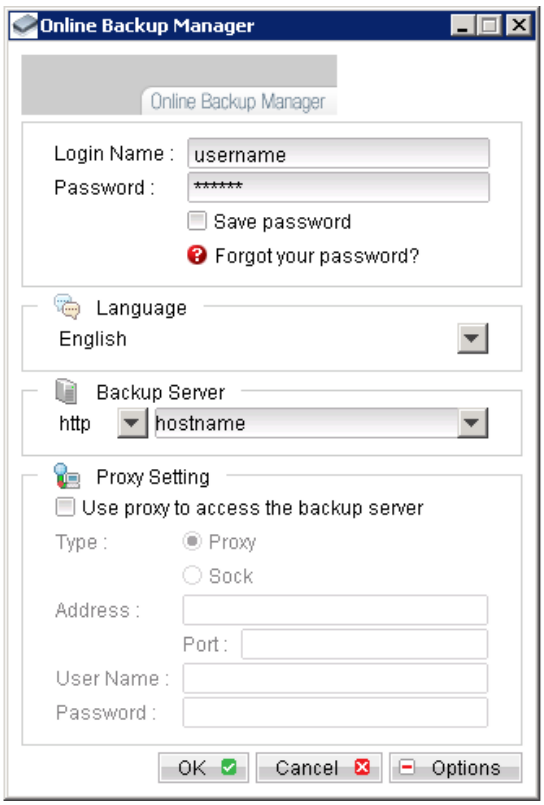
Important:
Serious problem may occur if the configuration files are incorrectly modified; it may prevent the virtual machine from starting.

Please only perform the following procedures if you have in-depth knowledge on Hyper-V management.

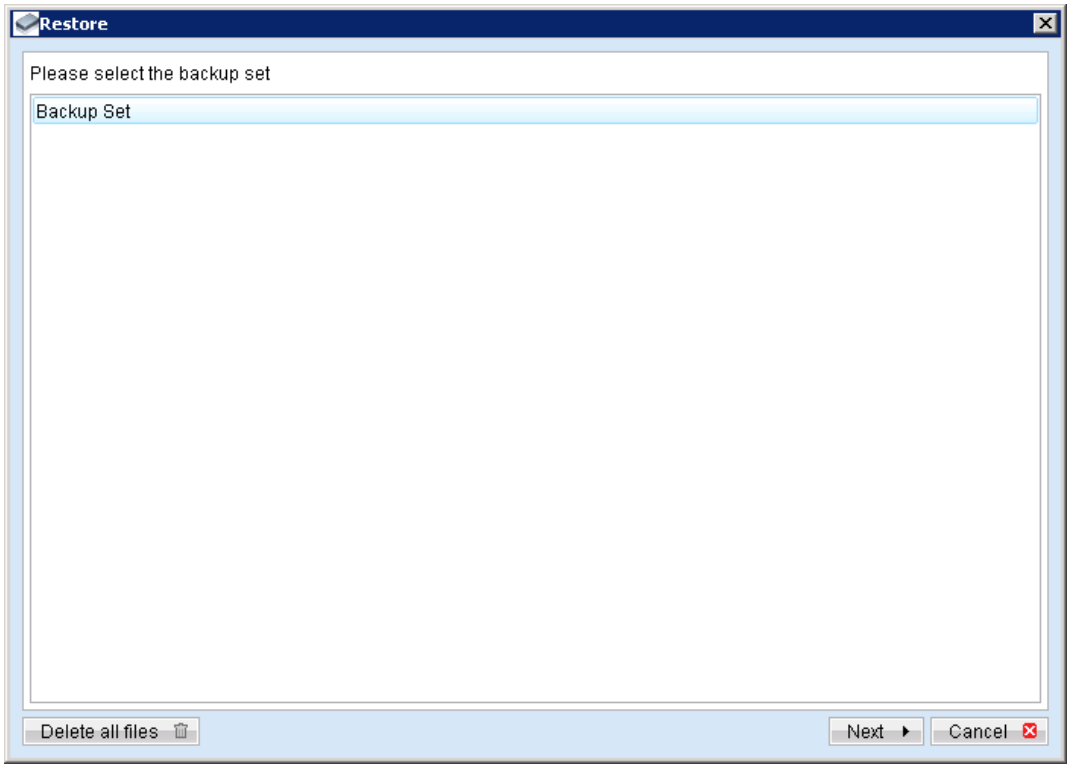
14.1.1.6 How to restore individual virtual disk to original VM

1. Open Hyper-V Manager.
2. Shutdown the VM to be restored to.
3. Login to the backup application's user interface.



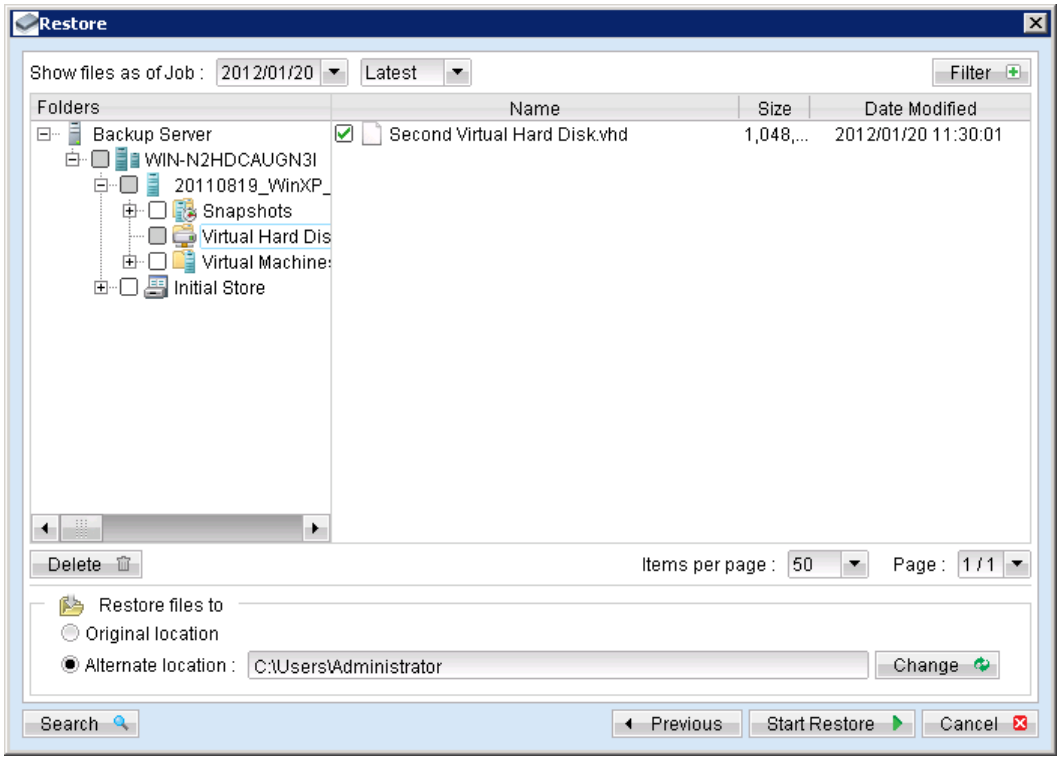


4. Select the [Restore] button and the corresponding backup set.



5. Select [Alternate location], then select the virtual disk to be restored.

   Restore of individual virtual disk is only supported for restore to [Alternation location].

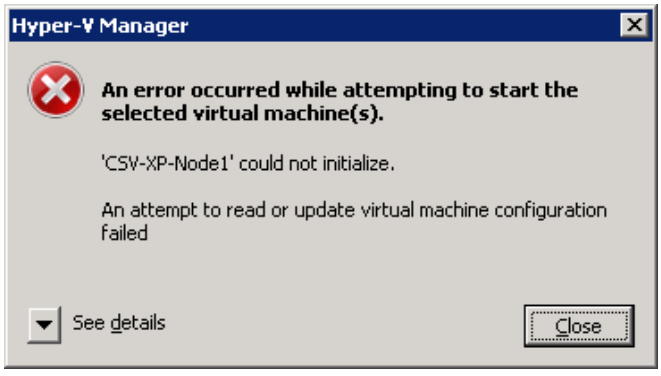


6. Click [Change]; select the directory path where the virtual disk was originally backed up from.

7. Click the [Start Restore] button to begin the restore process.

8. Start the virtual machine after the restore process is completed.

Important:
If the following error is displayed during the startup, please remove the Saved State of the corresponding VM.

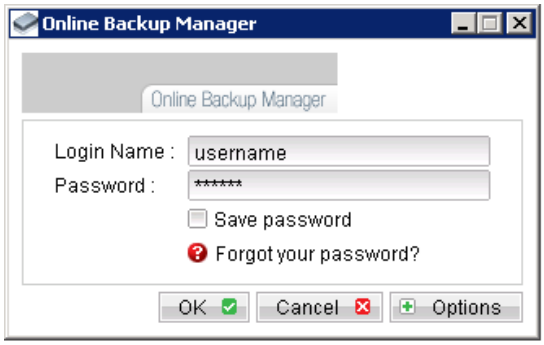

Hyper-V Manager
An error occurred while attempting to start the selected virtual machine(s).
'CSV-XP-Node1' could not initialize.
An attempt to read or update virtual machine configuration failed
See details
Close

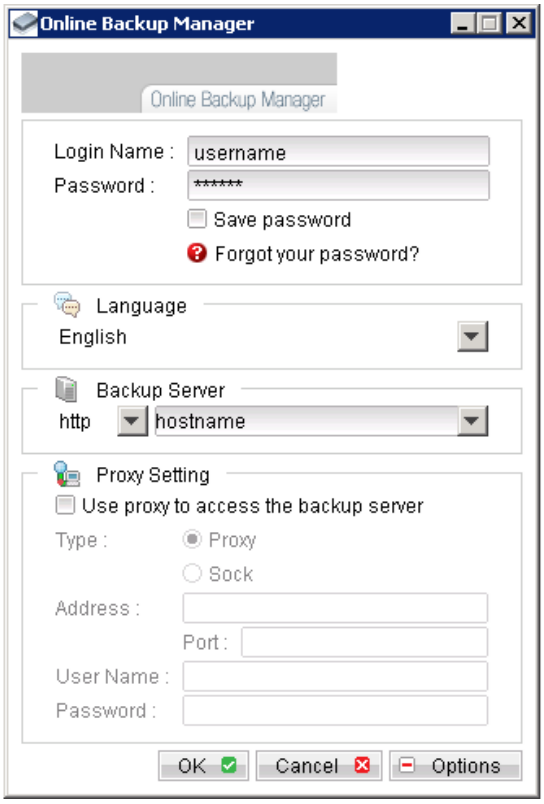
In Hyper-V Manager, right click on the corresponding VM and select [Delete Saved State], start the VM again afterward.

14.1.2.6 How to restore individual virtual disk to a different VM

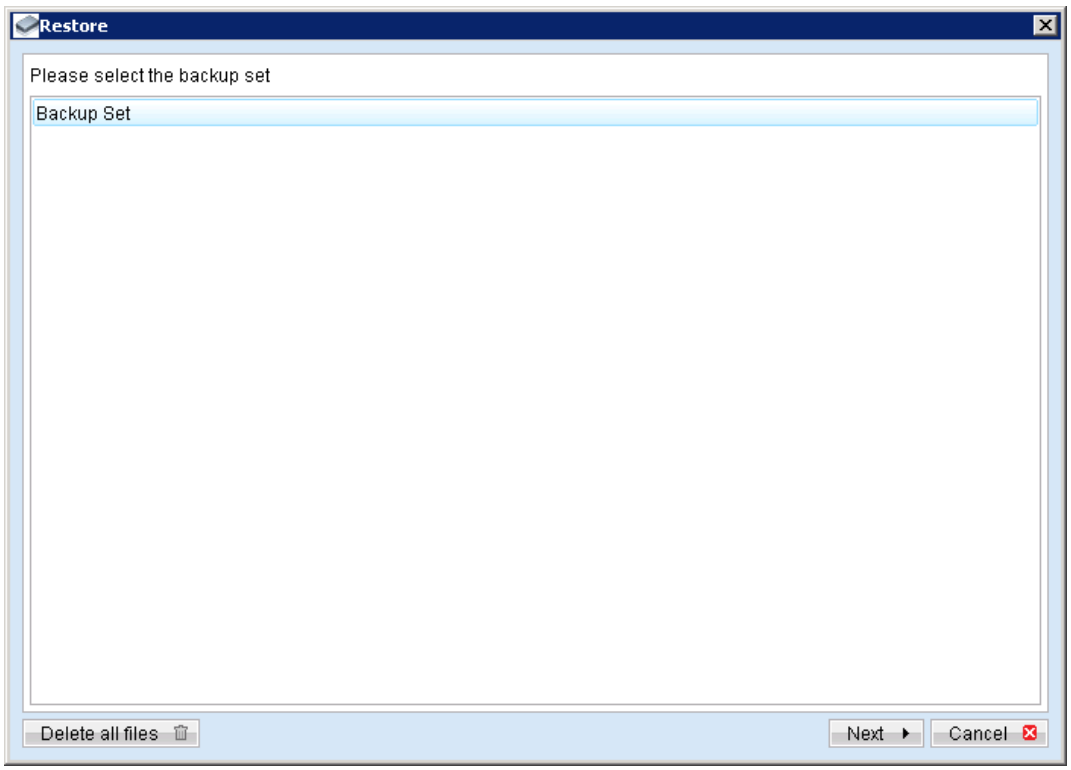
Important:
Restore of individual virtual disk to a different virtual machine is only supported for virtual disk with no snapshot.

1. Login to the backup application's user interface.



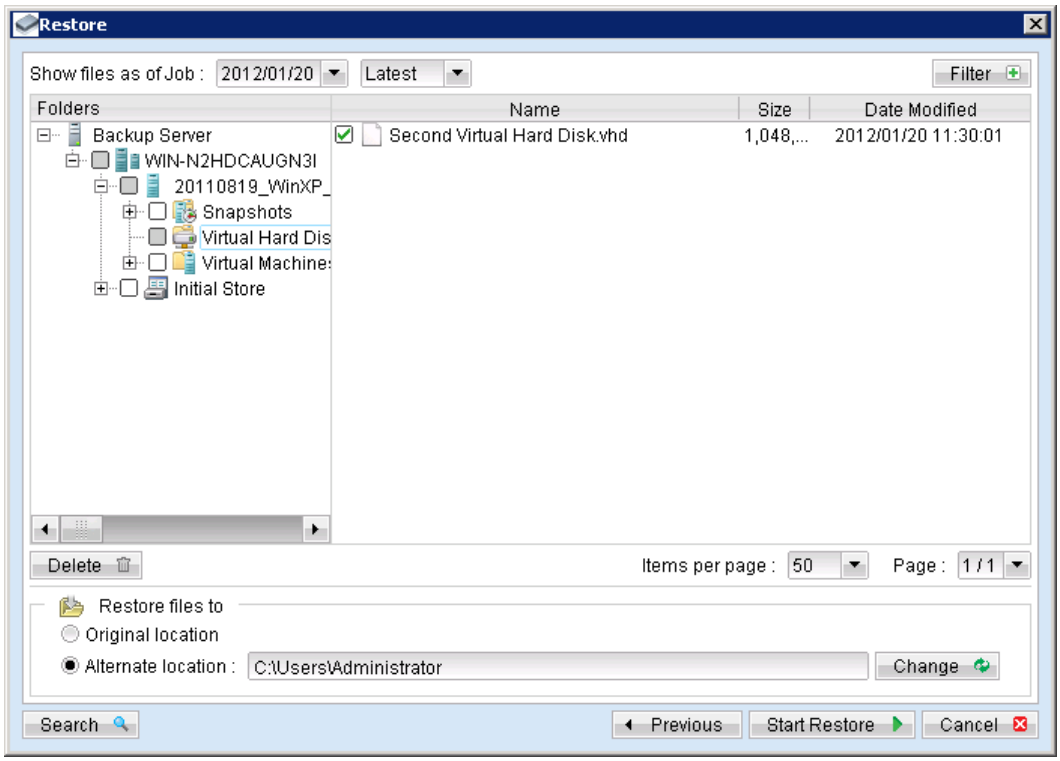


2. Select the [Restore] button and the corresponding backup set.



3. Select [Alternate location], then select the virtual disk to be restored.

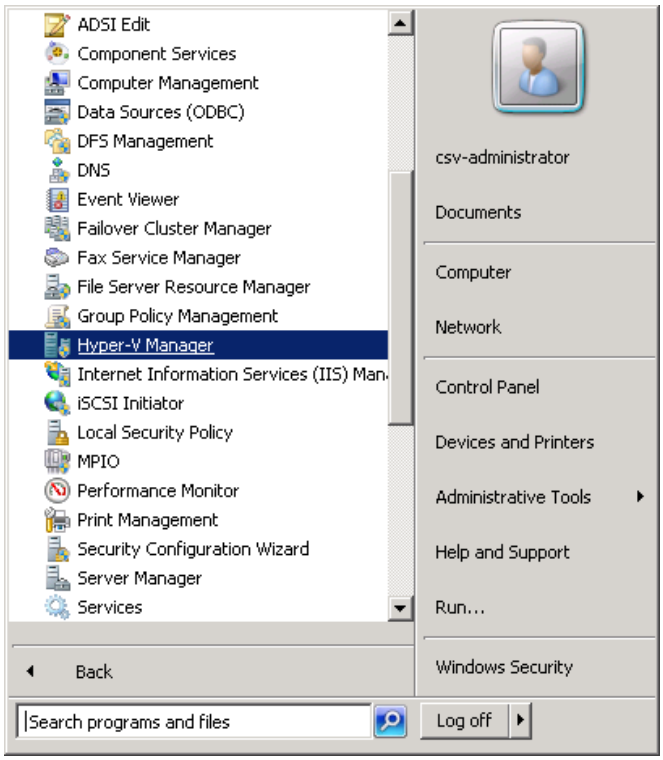
   Restore of individual virtual disk is only supported for restore to [Alternation location].



4. Click [Change] to select the location where the virtual disk should be restored.

5. Click the [Start Restore] button to begin the restore process.

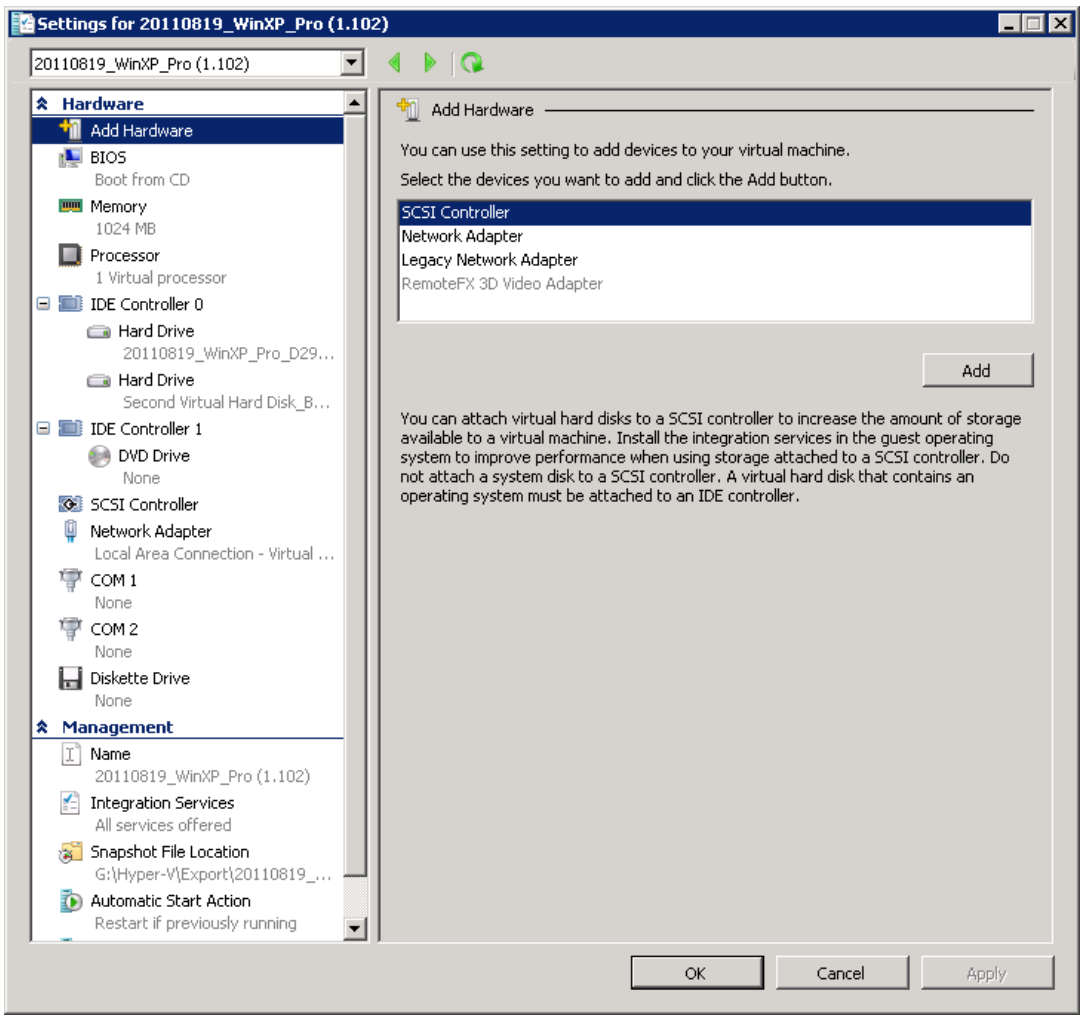
6. When the restore process is completed, open Hyper-V Manager.



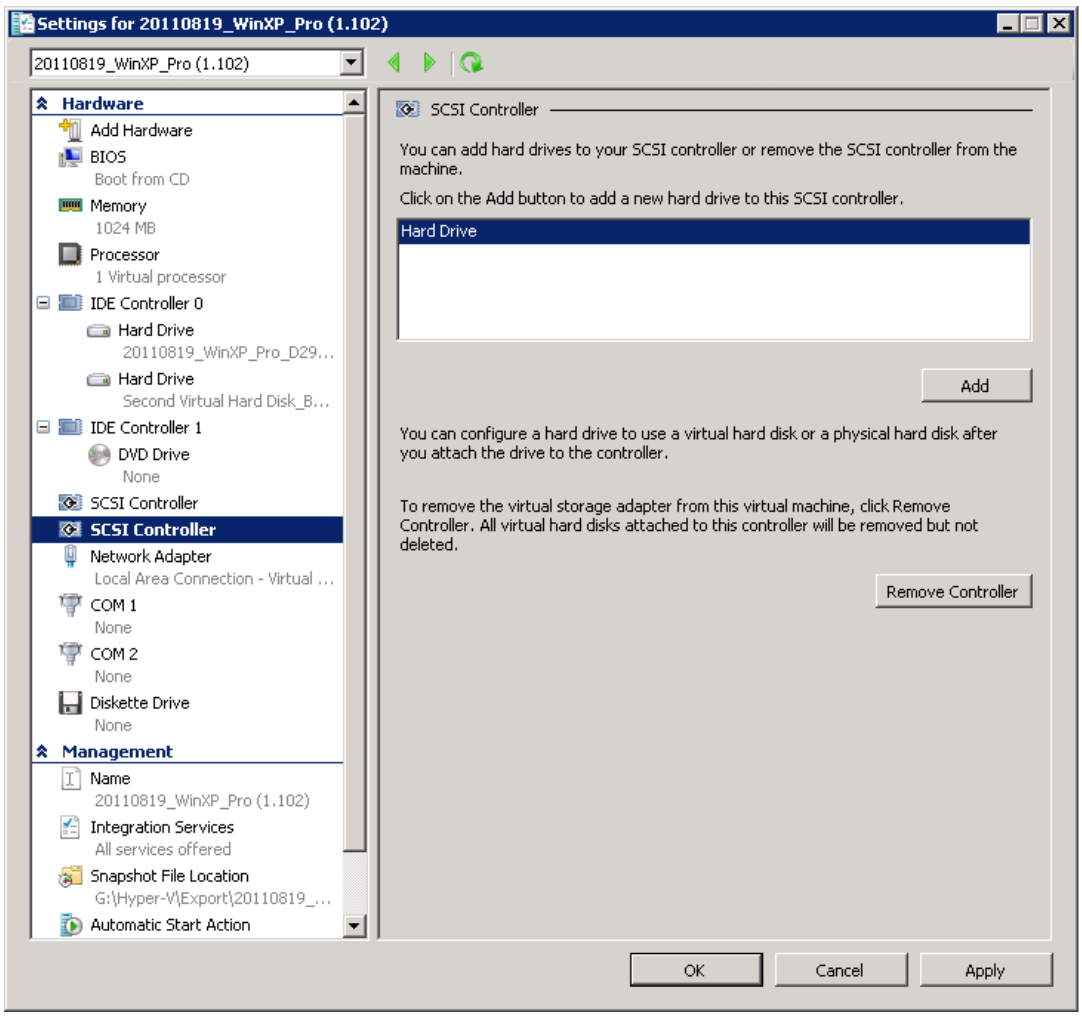
7. Under Virtual Machines, powers down the corresponding virtual machine to be restored to.

8. Select [Setting] to add the restored virtual disk to the VM.

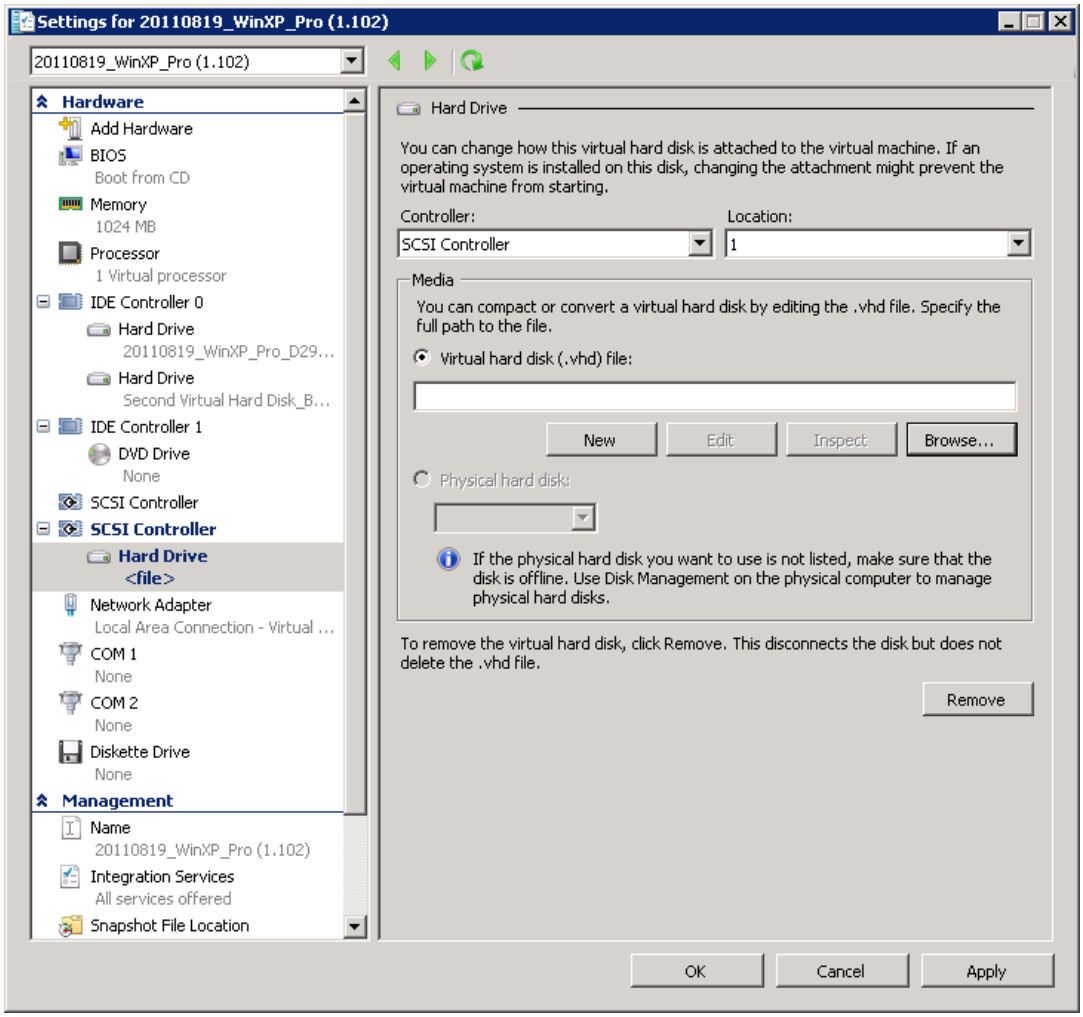
9. Select [Add Hardware], [SCSI Controller] and press the [Add] button.



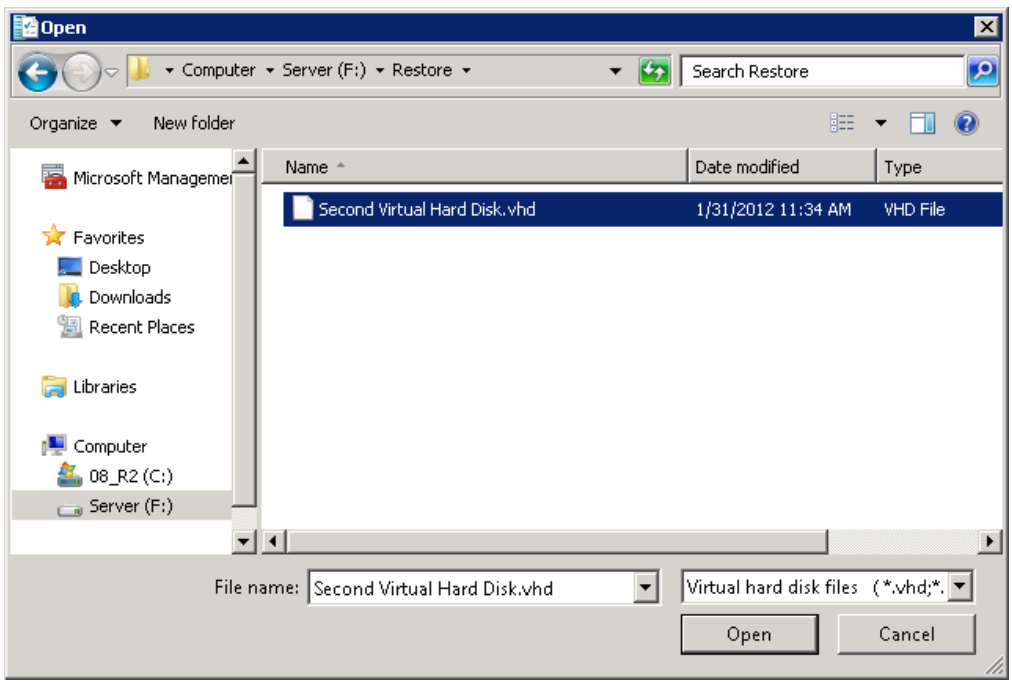
10. Select [Hard Drive] and press the [Add] button.



11. Select the corresponding [Controller] and [Location] setting.



12. Under Media, select [Browse] and browse to the newly restored virtual disk file.



13. Start the virtual machine.

14.2 Backup virtual machines running on Hyper-V Server (cluster environment)

14.2.1 Requirements and recommendations

Please ensure that the following requirements are met by all Hyper-V cluster nodes:

1. OBM version 6.7 or above is installed on all Hyper-V cluster nodes.
2. The Hyper-V management tools are installed on all Hyper-V cluster nodes.
3. Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation.
4. It is recommended that the temporary directory have disk space of at least 50% of the largest sized virtual machine to be backed up.
5. For backup of virtual machine with snapshot, backup of the whole VM instead of individual disk is highly recommended.
6. Special attentions must be paid to the license requirement for backup of all VM in the cluster. Refer to the following section for details.

14.2.2 Limitations

The following are limitations of the MS VM backup module:

1. Virtual machines backed up with the MS VM backup module can only be restored to the original Hyper-V server.
2. Backup of virtual machine with pass through disk (directly attached physical disk) is not supported.
3. For virtual machine with snapshot, the restoration process for individual virtual disk requires manual editing of VM configuration files.

   In-depth knowledge on Hyper-V is required.
4. For backup of individual virtual disk, the restored virtual machine does not support the reversion of previous snapshots, if the snapshot contains disks which are not previously backed up by OBM

5. The virtual machine cannot start up if the operating system virtual disk is not restored.

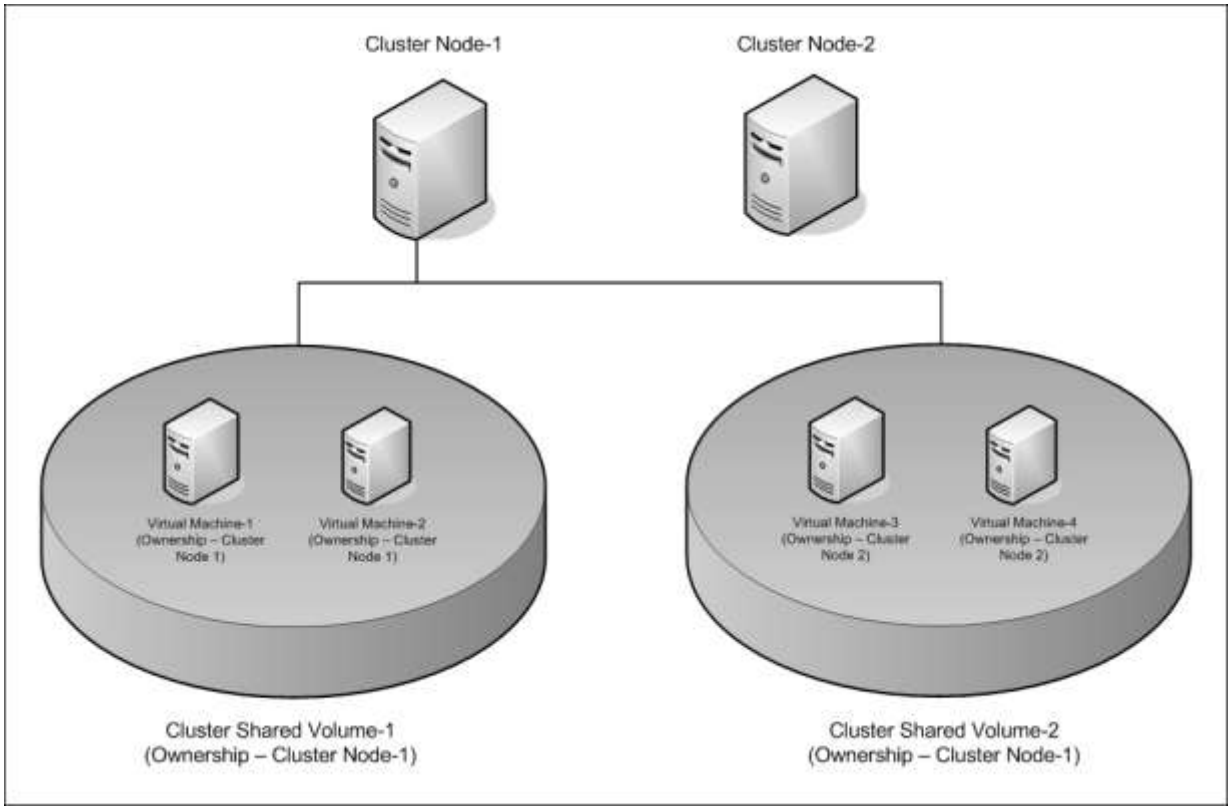
6. OBM installation on each node can only backup VMs owned by that particular node.

7. OBM installation on each node can only backup VMs residing on Cluster Shared Volume own by that particular node.

To give a better illustration of point 5 and 6, please refer to the following example:

Initial Setup
2 nodes cluster environment with 2 cluster shared volume (CSV) and 4 virtual machines.

Cluster Node	**Cluster Resource Owned**
Cluster Node-1	Cluster Shared Volume-1 Cluster Shared Volume-2 Virtual Machine-1 Virtual Machine-2
Cluster Node-2	Virtual Machine-3 Virtual Machine-4


Cluster Node-1
Cluster Node-2
Virtual Machine-1 (Ownership – Cluster Node 1)
Virtual Machine-2 (Ownership – Cluster Node 1)
Virtual Machine-3 (Ownership – Cluster Node 2)
Virtual Machine-4 (Ownership – Cluster Node 2)
Cluster Shared Volume-1 (Ownership – Cluster Node-1)
Cluster Shared Volume-2 (Ownership – Cluster Node-1)

OBM installation on Cluster Node-1
Only Virtual Machine-1 and Virtual Machine-2 can be backed up, as Virtual Machine-3 and Virtual Machine 4 are owned by Cluster Node-2.

OBM installation on Cluster Node-2
No virtual machine can be backed up as both cluster shared volumes are owned by Cluster Node-1.

In the above setup, Virtual Machine-3 and Virtual Machine-4 cannot be backed up.

To backup all 4 virtual machines within the cluster environment
Option 1 - Switch ownership of Cluster Shared Volume-2:

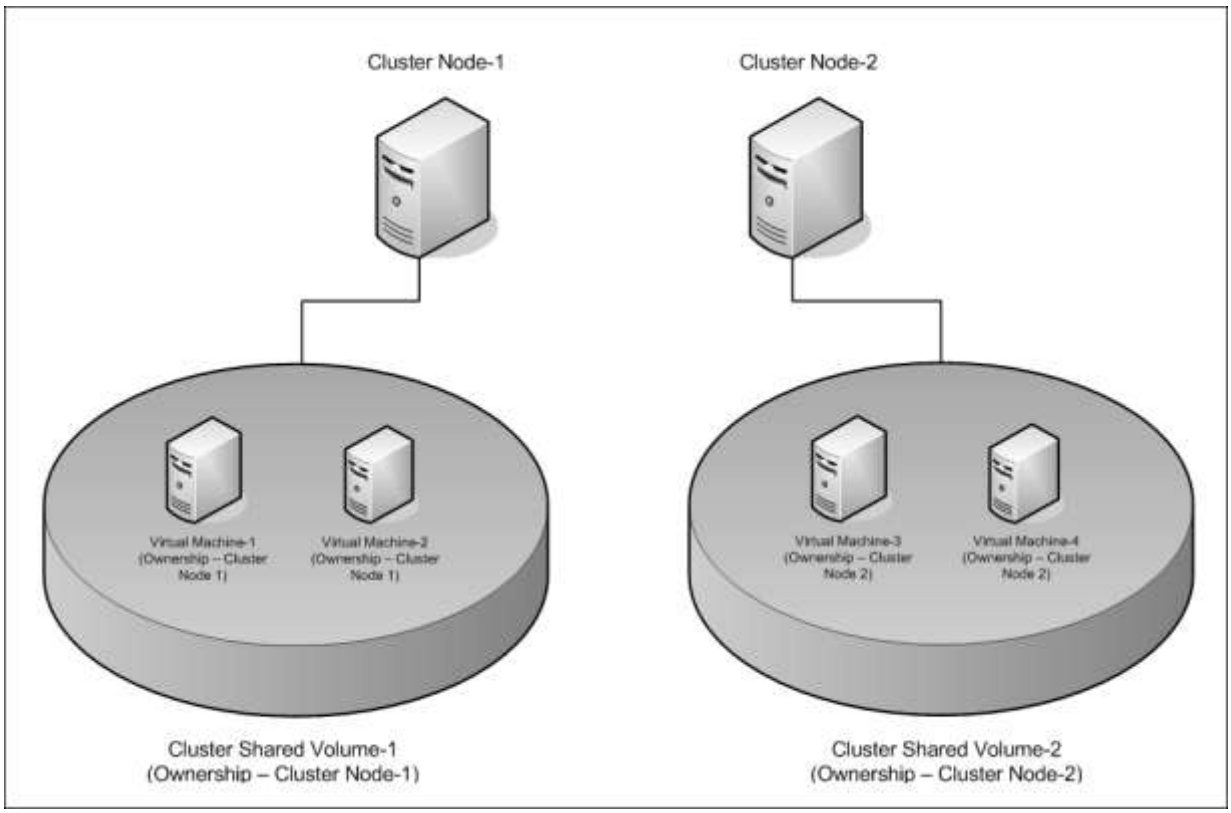
- Switch ownership of Cluster Shared Volume-2 to Cluster Node-2.
- Install OBM on both Cluster Node-1 and Cluster Node-2.
- Configuration backup of VMs on both node, where:

  Cluster Node-1 will backup Virtual Machine-1 and Virtual Machine-2.
  Cluster Node-2 will backup Virtual Machine-3 and Virtual Machine-4.

New Setup with Option 1 - Switch ownership of Cluster Shared Volume-2

Switch Cluster Shared Volume-2's ownership from Cluster Node-1 to Cluster Node-2.

Cluster Node	**Cluster Resource Owned**
Cluster Node-1	Cluster Shared Volume-1 Virtual Machine-1 Virtual Machine-2
Cluster Node-2	Cluster Shared Volume-2 Virtual Machine-3 Virtual Machine-4


Cluster Node-1
Cluster Node-2
Virtual Machine-1 (Ownership – Cluster Node 1)
Virtual Machine-2 (Ownership – Cluster Node 1)
Virtual Machine-3 (Ownership – Cluster Node 2)
Virtual Machine-4 (Ownership – Cluster Node 2)
Cluster Shared Volume-1 (Ownership – Cluster Node-1)
Cluster Shared Volume-2 (Ownership – Cluster Node-2)

Important:
Depending on your backup source selection, you may need to update the backup source setting when a change of ownership occurs for any virtual machine (e.g. VM fail over from Cluster Node-1 to Cluster Node-2).

Option 2 - Switch ownership of Virtual Machine-3 and Virtual Machine-4 (only suitable for Active-Passive cluster environment):

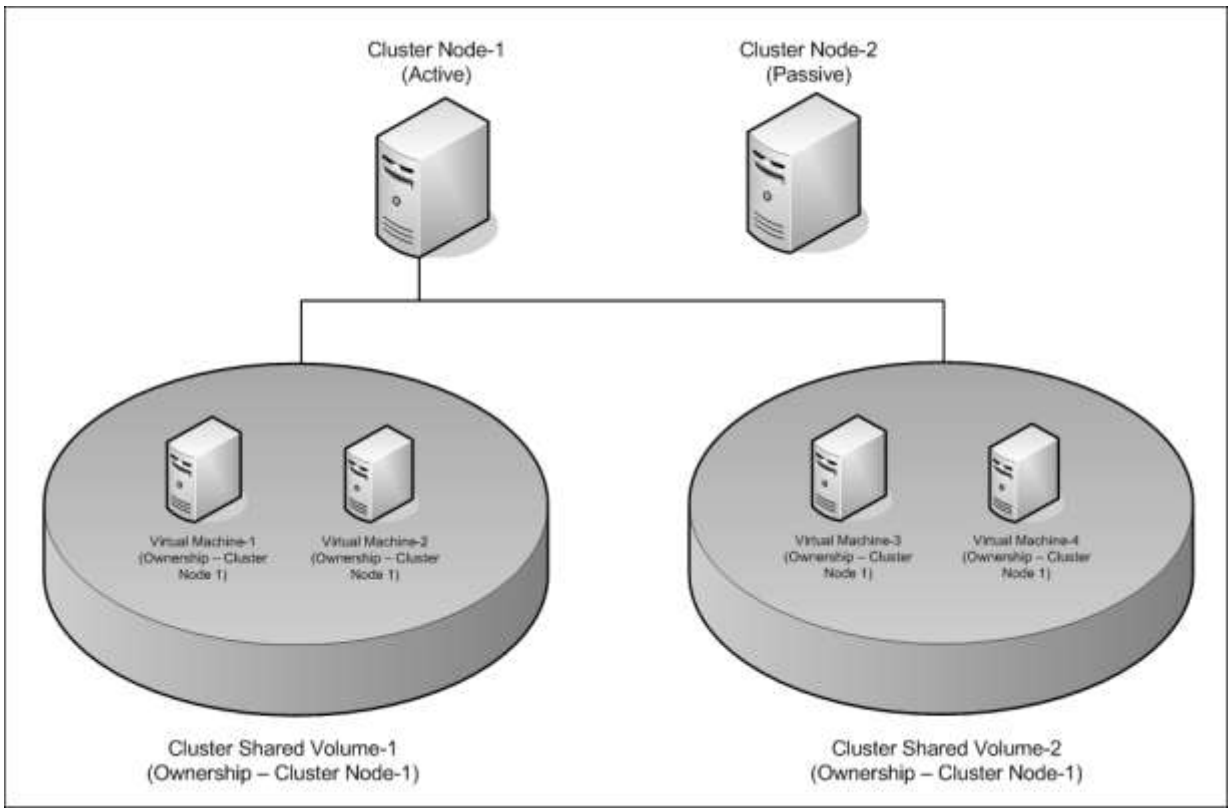
- Switch ownership of Virtual Machine-3 and Virtual Machine-4 to Cluster Node-1.
- Install OBM on Cluster Node-1.
- Configuration backup of VMs on Cluster Node-1 where, Cluster Node-1 will backup all 4 VMs.

New Setup with Option 2 - Switch ownership of Virtual Machine-3 and Virtual Machine-4

Switch all cluster resources to Cluster Node-1, making Cluster Node-2 a passive node.

Cluster Node	Cluster Resource Owned
Cluster Node-1 (Active)	Cluster Shared Volume-1 Cluster Shared Volume-2 Virtual Machine-1

	Virtual Machine-2 Virtual Machine-3 Virtual Machine-4
Cluster Node-2 (Passive)	



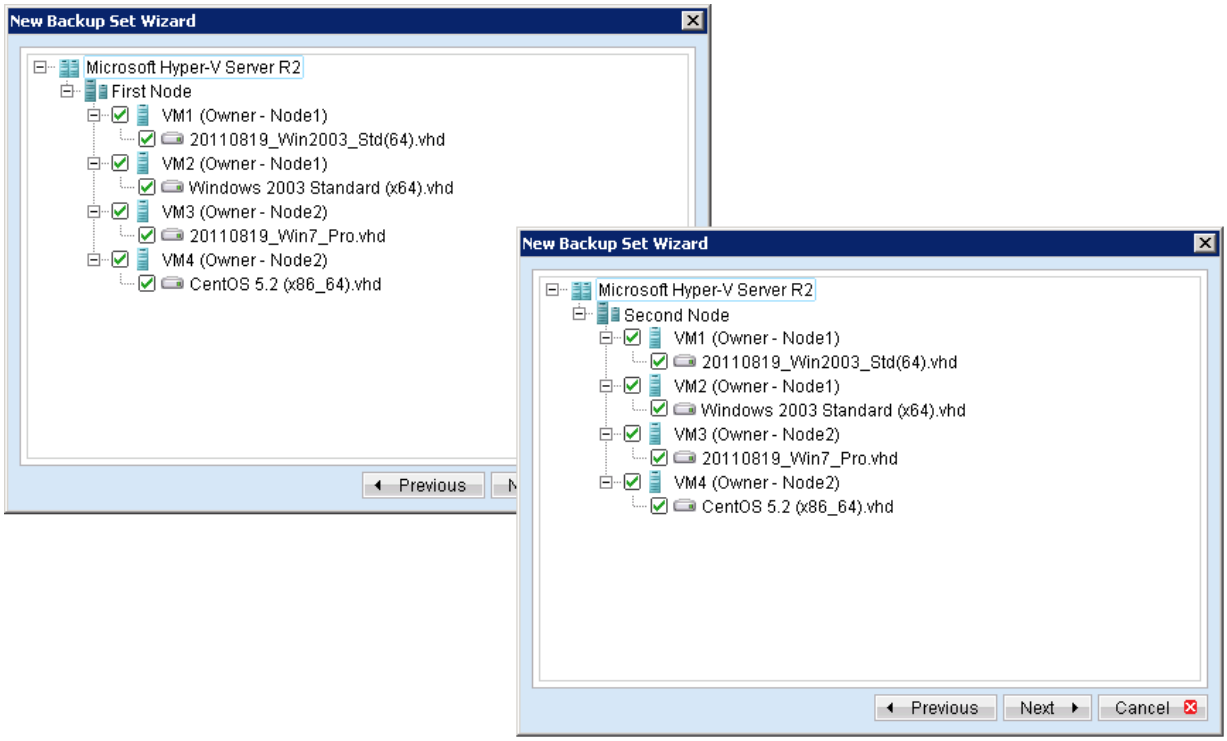
Important:
With option 2, OBM must be installed, and the backup must be re-configured on Cluster Node-2 (using the existing backup set) when a change of ownership occurs for any cluster resources (e.g. Cluster Node-1 failing).

14.2.3 License requirement to backup all virtual machines in a cluster

There are two types of configuration which you can used to backup all VMs within a cluster. The license requirements for these setups are different.

Method 1 - Select all VMs for each cluster node specific backup set

For the simplest method to backup all VMs, in each cluster node specific backup set, select all VMs as backup source.



With this method, all VMs are backed up regardless of their ownership status.

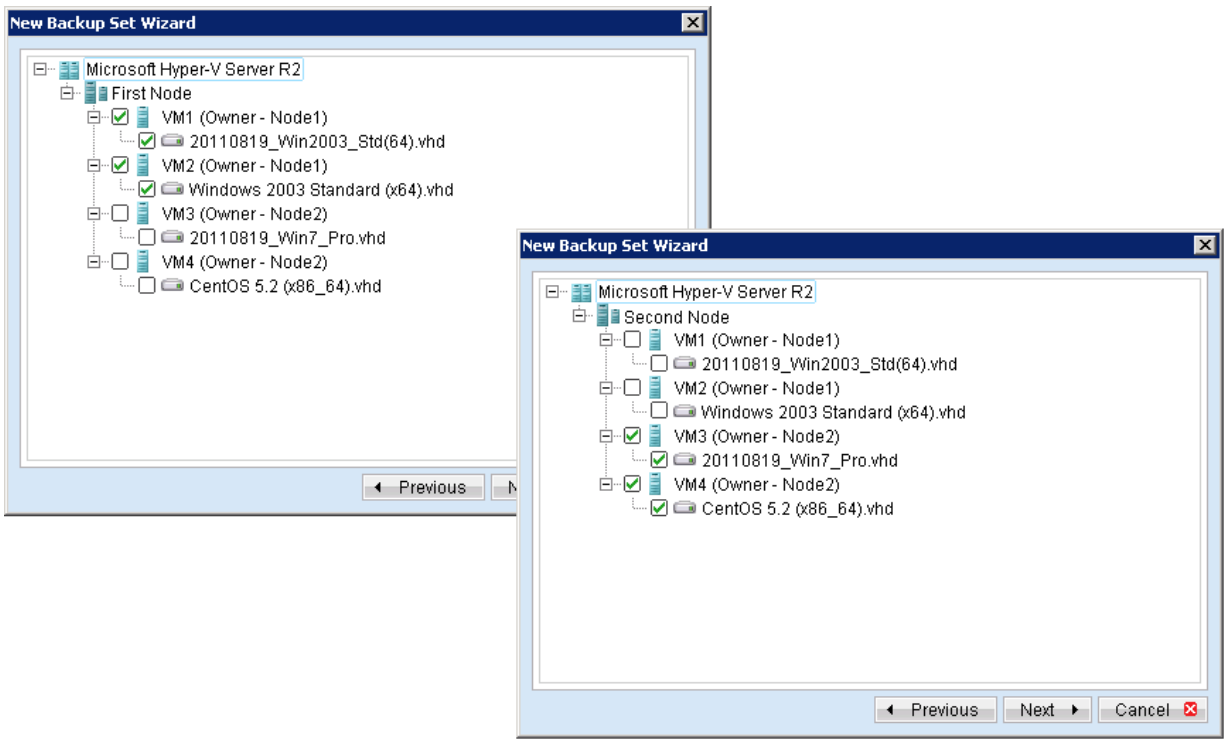
Note:
Only VMs that own by each particular node will be backed up by its respective backup set, there will be no duplicate backup.

The drawback for this method is, extra standby license will be required.

For example, in a 2 nodes cluster environment, with 4 total VMs, 8 VM licenses will be required (e.g. Total number of VMs x Total number of cluster nodes).

Method 2 - Select only VMs of the cluster node for each node specific backup set

For cost efficiency, in each cluster node specific backup set, select only VMs that currently belong to the particular node.



For example in a 2 nodes cluster environment, with 4 total VMs, 4 VM licenses will be required (e.g. total number of VMs).

The drawback for this method is, backup source of each node specific backup set must be updated whenever a change of ownership occurs, for any VM.

For example when the ownership of VM1 changes from Node1 to Node2, you must update Node1's specific backup source (e.g. unselect VM1 from Node1 backup set's backup source and vice versa for Node2 backup set's backup source).

The following table summarizes the benefits and drawbacks of the two configurations:

Type	Benefits	Drawbacks
Select all VMs for each cluster node's backup set	Simple setup, all VMs are backed up regardless of their ownership status. Less maintenance required.	More standby licenses are required. License Requirement - Total number of VMs x Total number of cluster nodes
Select only VMs of the cluster node for each node's specific backup set	Fewer licenses are required. License Requirement - Total number of VMs	Backup source of each node's specific backup set must be updated whenever a change of ownership occurs for any VM.

14.2.4 Overview

The following steps are performed during a backup job:

1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Commands are issued to the hypervisor to create snapshot (e.g. memory dump) of the virtual machine with Volume Shadow Copy.

   Important:
   The corresponding virtual machine will be paused during the snapshot process, and resume when the snapshot is completed.

   Do not attempt to start the virtual machine while it is in the saving state. The snapshot created may be invalid.

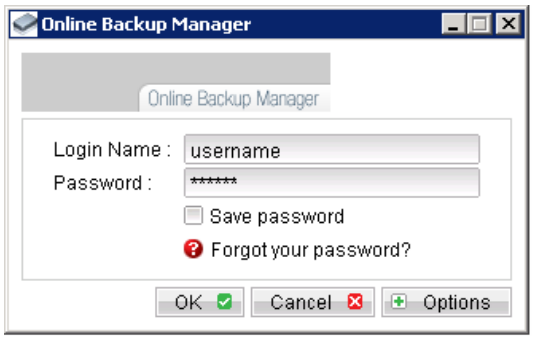
   Furthermore, the corresponding virtual machine uptime will also be reset to 00:00:00 in the Hyper-V Manager
4. After generating all files, the files are copied to the temporary spool path and upload to OBS.
5. Commands are issued to the hypervisor to remove the Volume Shadow Copy snapshot created.
6. Backup completed successfully.

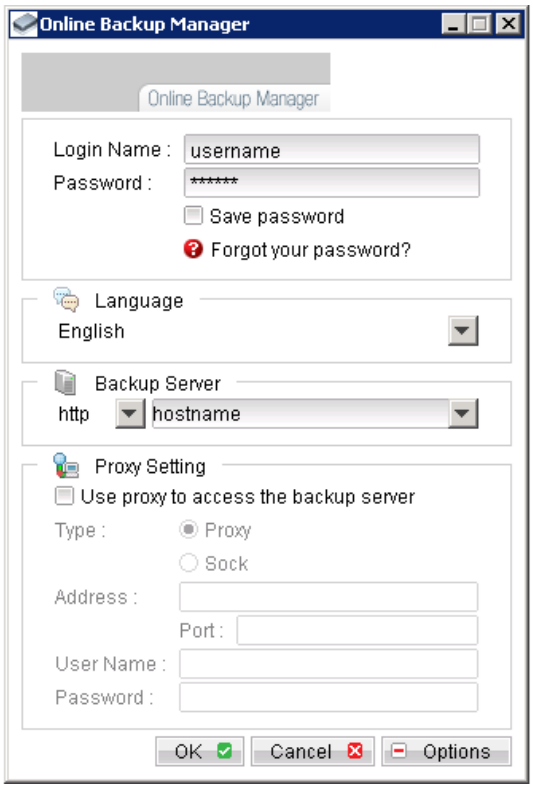
14.2.5 How to backup Microsoft virtual machines in cluster environment

Refer to the following instructions to backup VM running on Microsoft Hyper-V Server in cluster environment:

1. Install OBM on all Hyper-V cluster nodes.

2. Login to the backup application's user interface.



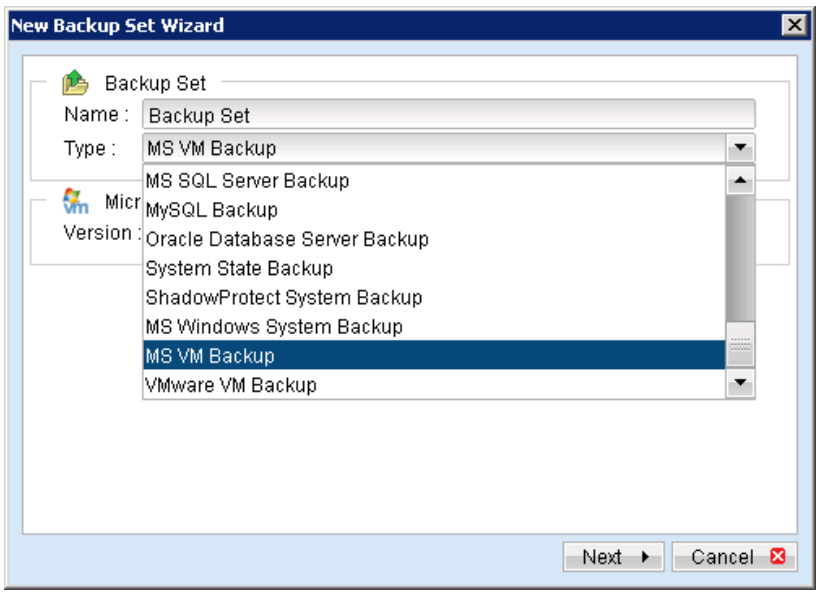


3. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

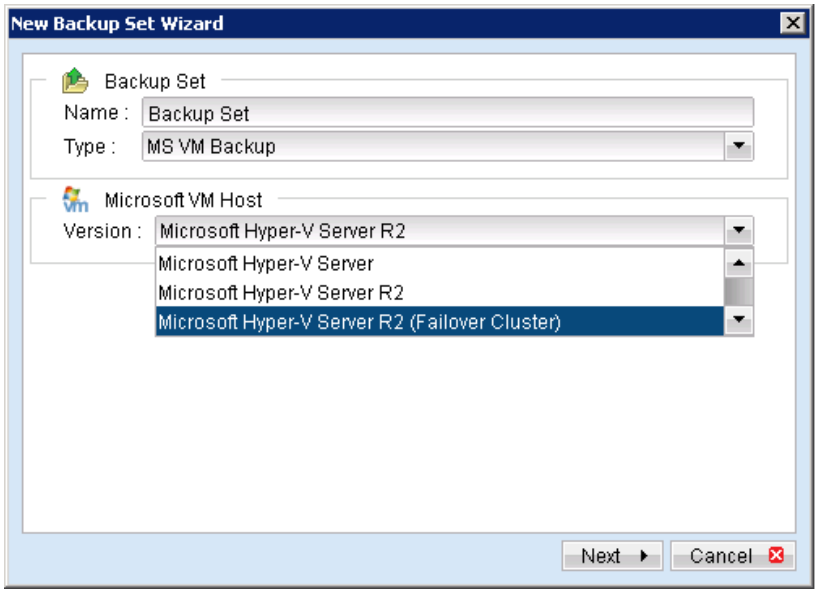
4. Create a separate MS VM Backup set for each cluster node.

   Important:
   Each cluster node must have its own unique MS VM backup set.

5. Select [MS VM Backup] from the backup set type dropdown menu.



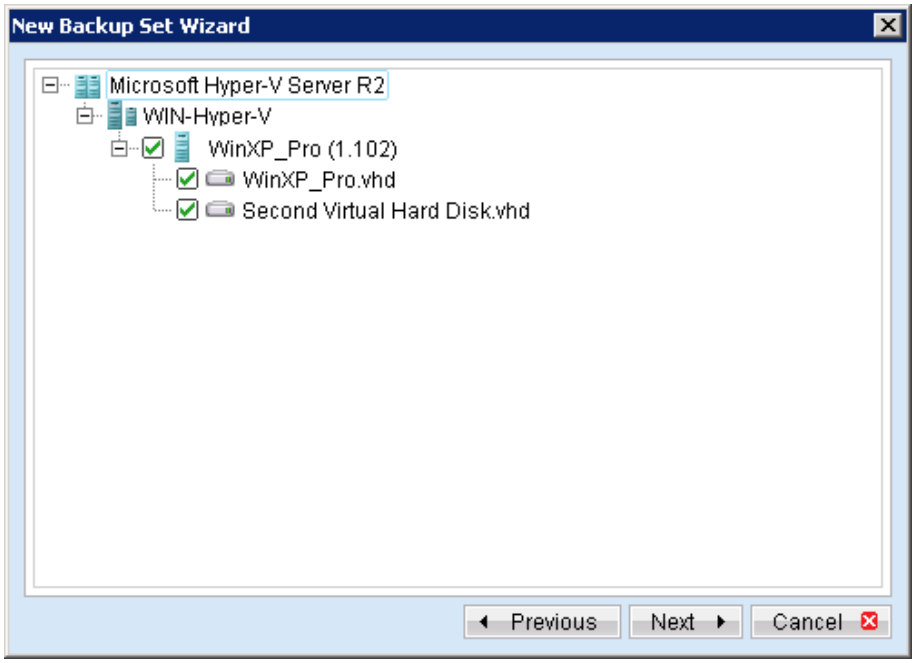
6. Select [Microsoft Hyper-V Server R2 (Failover Cluster)].



7. Select [Next] to proceed.

8. In the backup source selection screen, select the virtual machine for backup.

   To backup all VMs within the cluster setup, select all VMs listed.

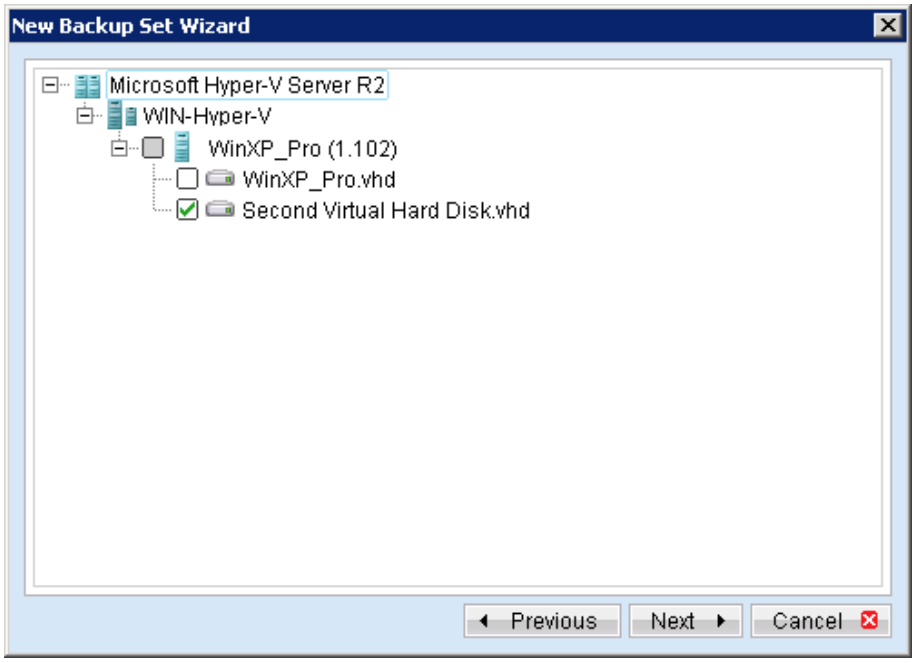


Important:
Even with all VMs selected for backup, only VM that belong the current node will be backed up.

VMs own by other cluster node will be skipped automatically.

Also, special attentions must be paid to the license requirement for backup of all VM in the cluster. Refer to the above section for details.

9. Alternatively, select individual virtual disk for backup by expanding the corresponding VM sub tree.



10. Configure a backup schedule for unattended backups.

Note:
Multiple backup schedules of different types can be configured for the same backup set

11. Select an encryption setting for your backup set.

12. Press the [OK] button to complete the configuration of backup set.

13. Scheduled backup will run automatically at the configured schedule time.

14. Perform the same setup on each cluster node.

15. Click [Backup] button on the left panel to perform a backup immediately.

Important:
Please refer to the Limitation section above for limitation on the backup configuration.

14.2.6 How to restore Microsoft virtual machines in cluster environment

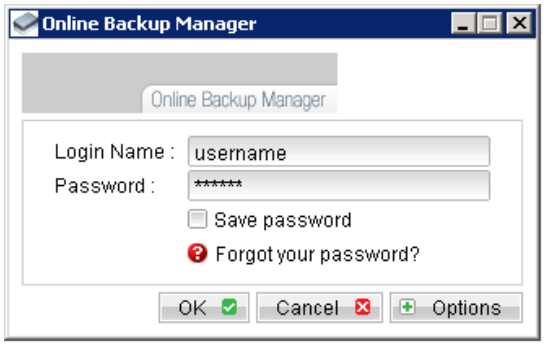
Refer to the following instructions to restore VM running on Hyper-V in cluster environment.

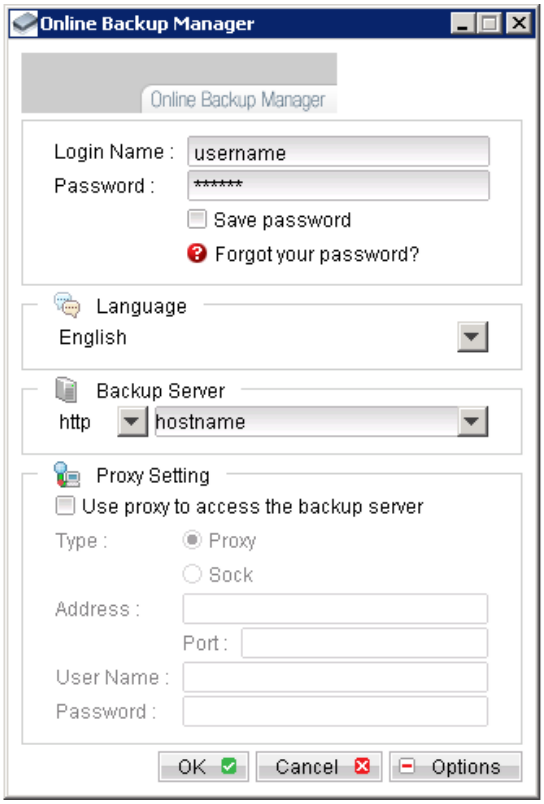
VM can be restored to the original location with the following condition:

- If the VM to be restored does not exist on the original hypervisor. The VM will be restored as a new virtual machine.
- If the VM to be restored still exist on the original hypervisor. The existing VM will be replaced by the backed up version.

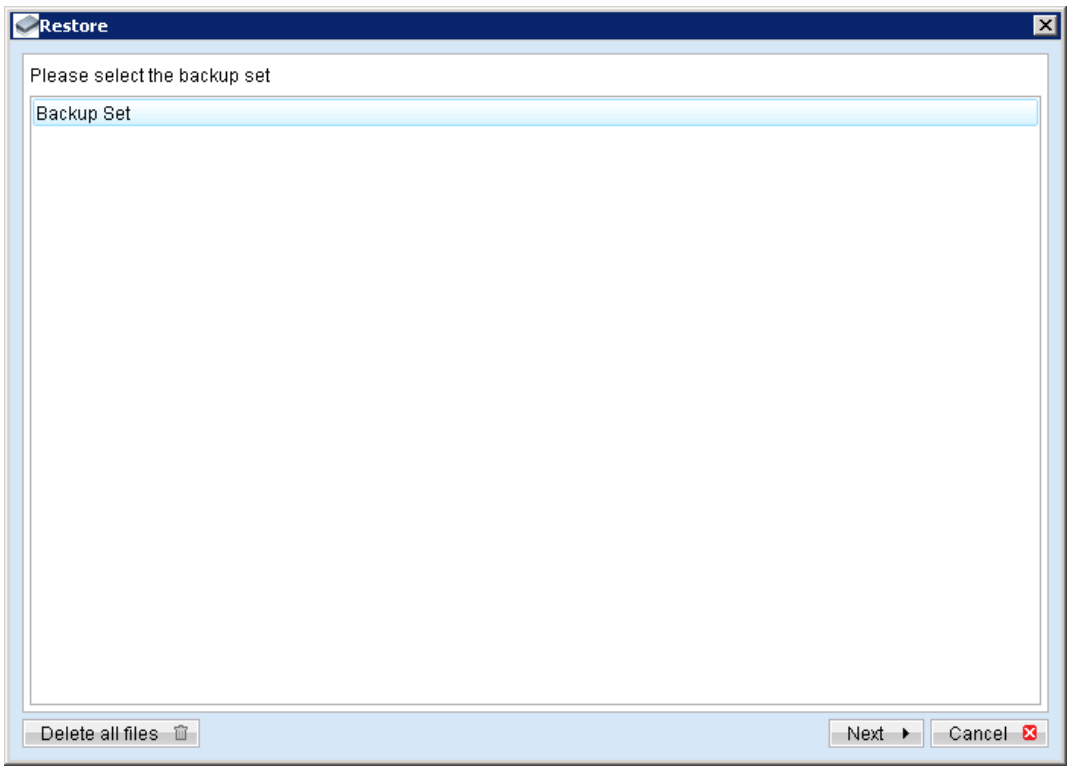
Important:
Virtual machine backed up with the MS VM backup module can only be restored to the original Hyper-V cluster node.

1. On the original Hyper-V cluster node, login to the backup application's user interface.

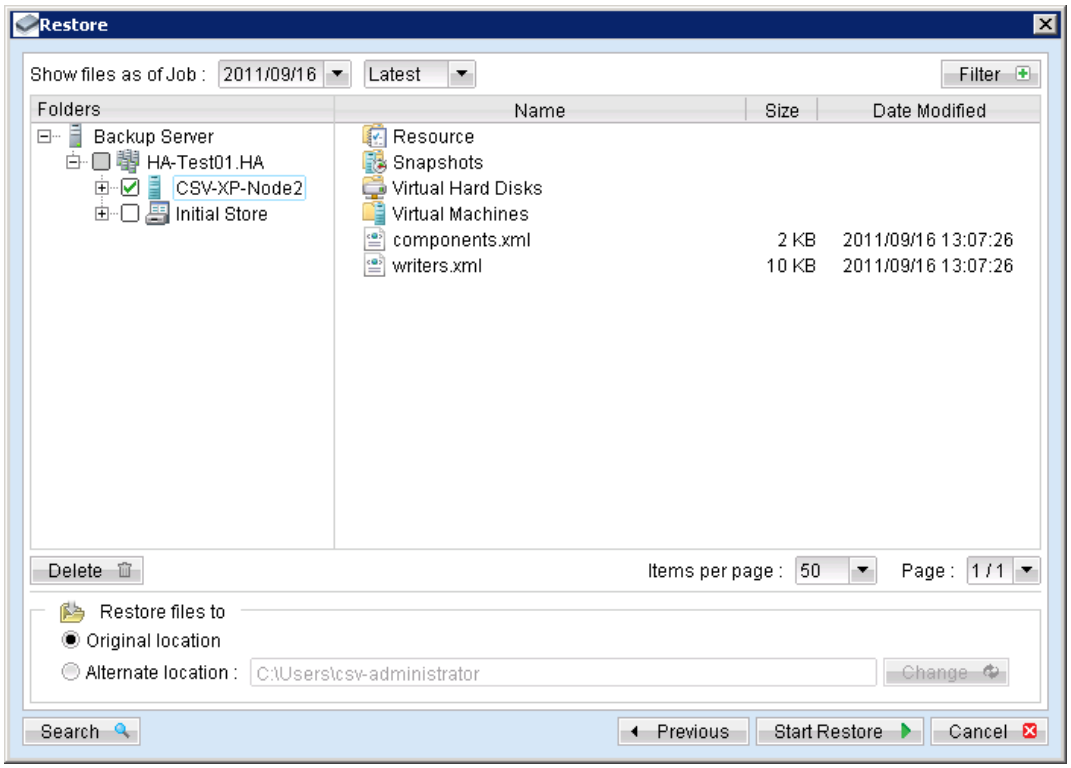




2. Select the [Restore] button and the corresponding backup set.



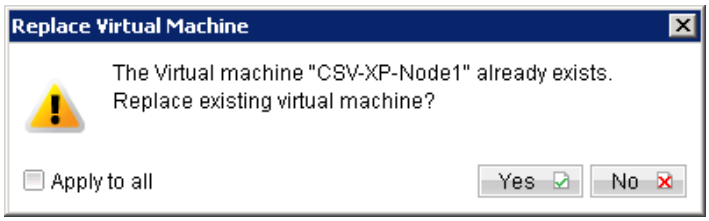
3. Select the virtual machines to be restored and choose [Original Location] for restore files to.



Note:
Select the Initial Store if you want to restore the Authorization Manager Security (role based access control) settings.

4. Click the [Start Restore] button to begin the restore process.

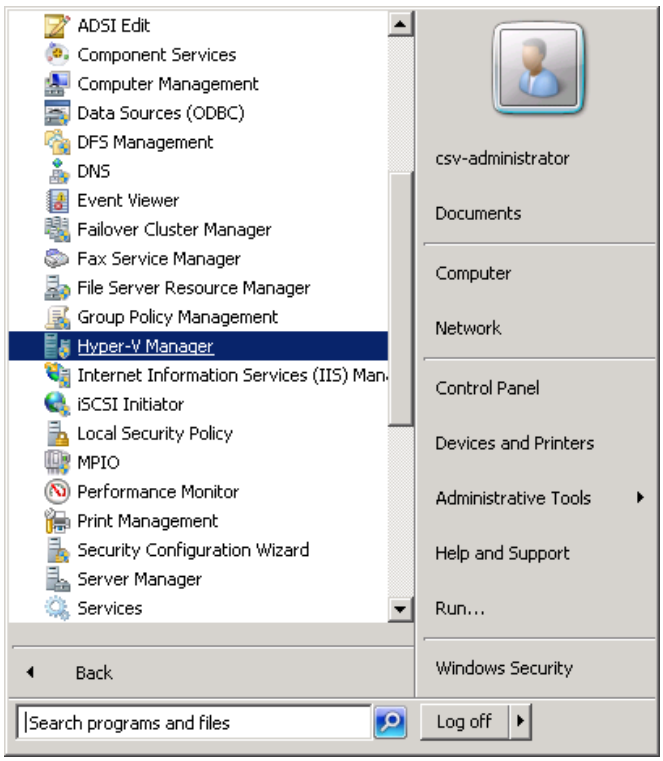
5. User will be prompted if a virtual machine selected to be restored exist on the hypervisor.



Important:
For restore of existing virtual machine (restoring a previous version), the existing virtual machine will be removed before the restore process begin.

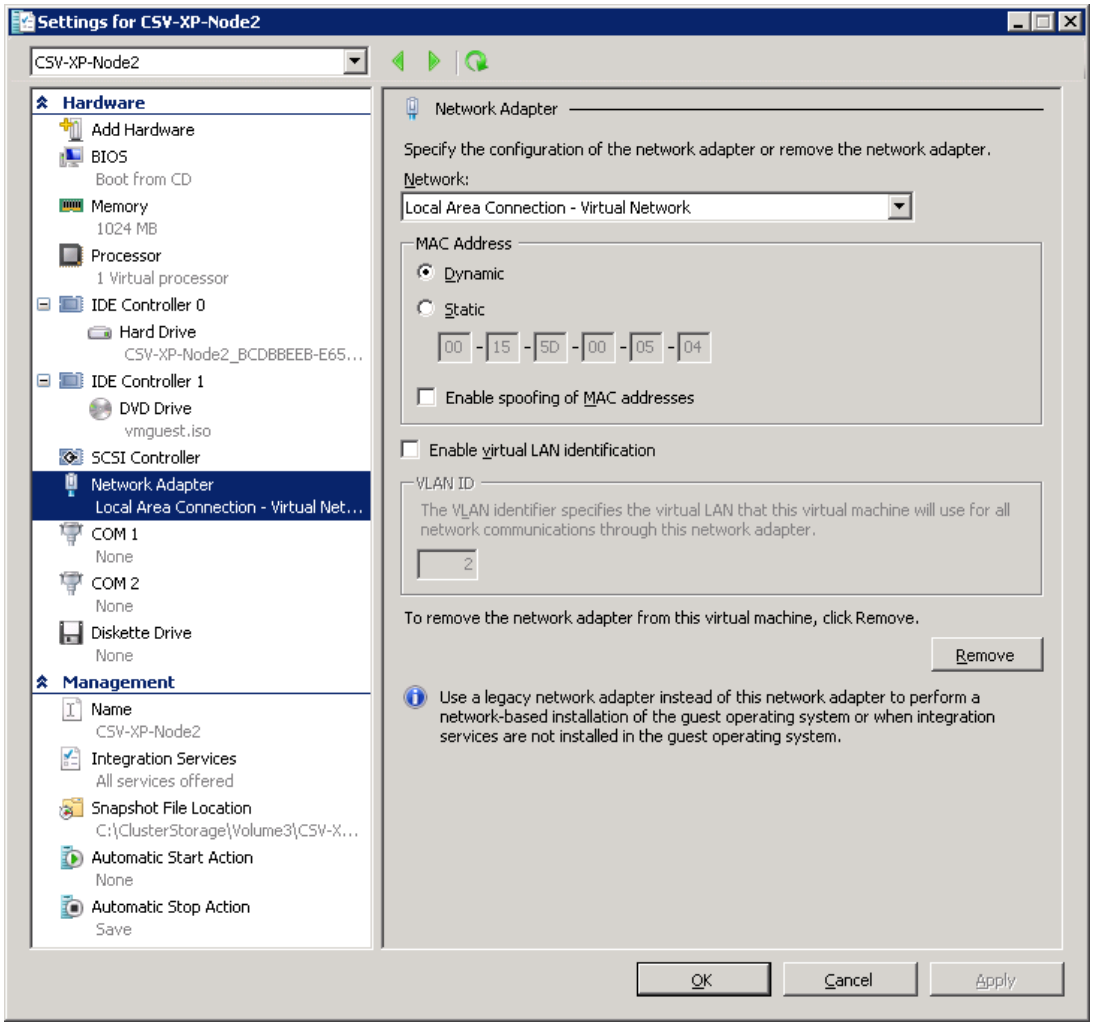
6. When the restore process is completed, the virtual machines will be restored to the original hypervisor.

7. Open Hyper-V Manager, click Start, Administrative Tools and click Hyper-V Manager.



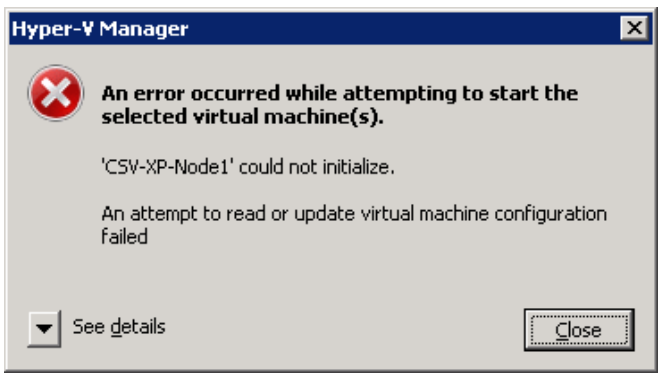
8. Under Virtual Machines, right click on the newly restored virtual machine, select [Setting].

9. Modify settings which may be conflicting with other existing virtual machines (e.g. network setting).



10. Start the virtual machine afterward.

Important:
If the following error is displayed during the startup, please remove the Saved State of the corresponding VM.


Hyper-V Manager
An error occurred while attempting to start the selected virtual machine(s).
'CSV-XP-Node1' could not initialize.
An attempt to read or update virtual machine configuration failed
See details
Close

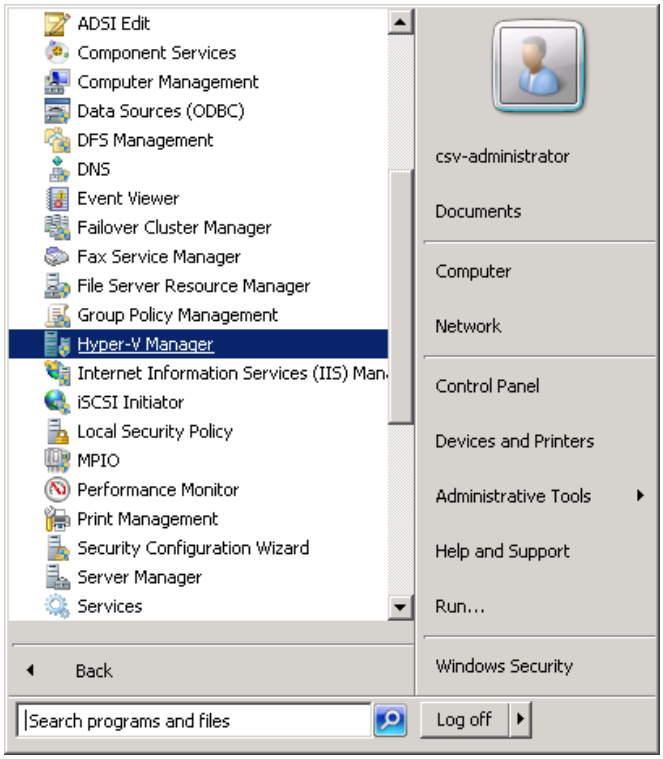
In Hyper-V Manager, right click on the corresponding VM and select [Delete Saved State], start the VM again afterward.

11. For any virtual disk that was not restored (e.g. original backup source did not include all virtual disks configured for the VM).

    Continue to the next steps for instruction to remove the missing virtual disk from the virtual machine's configuration.

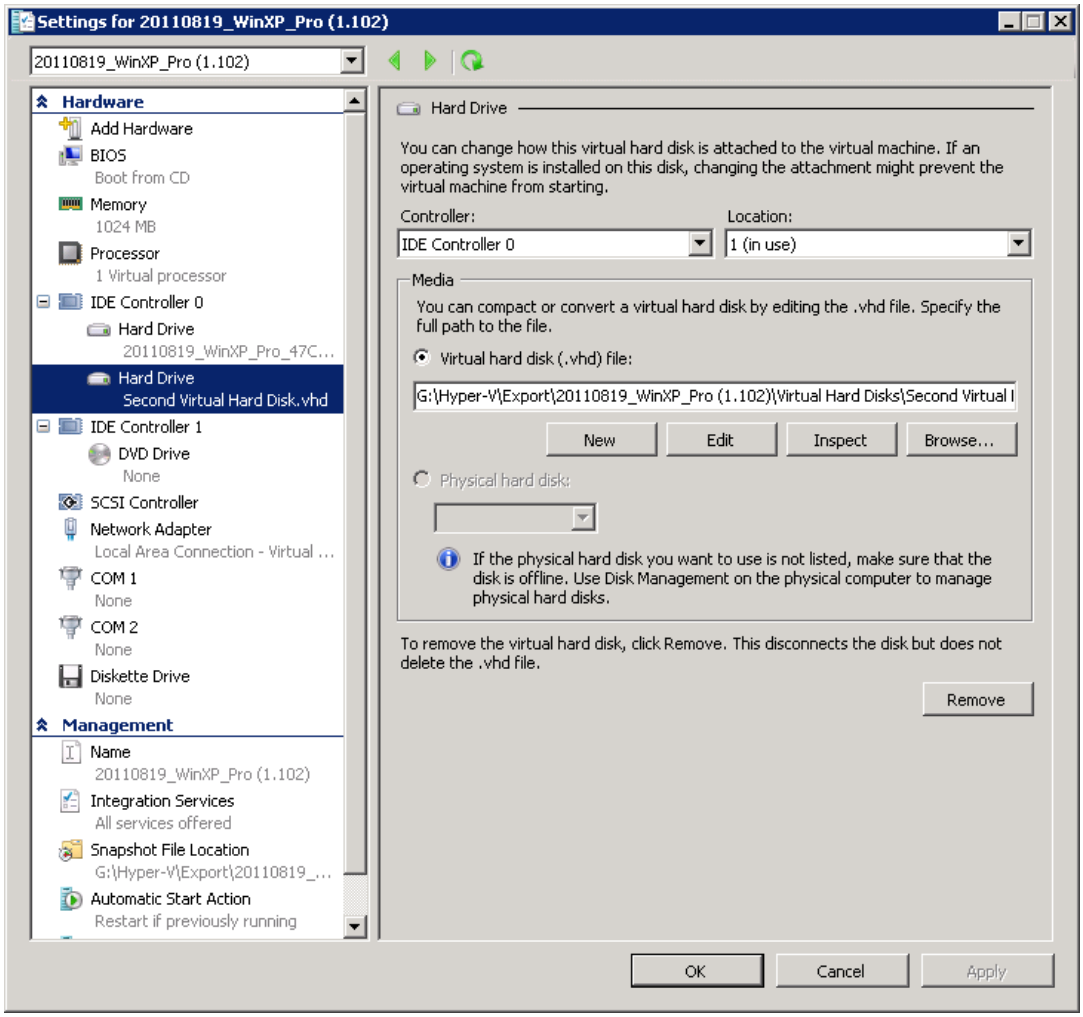
For original virtual machine with no snapshot

1. Open Hyper-V Manager.



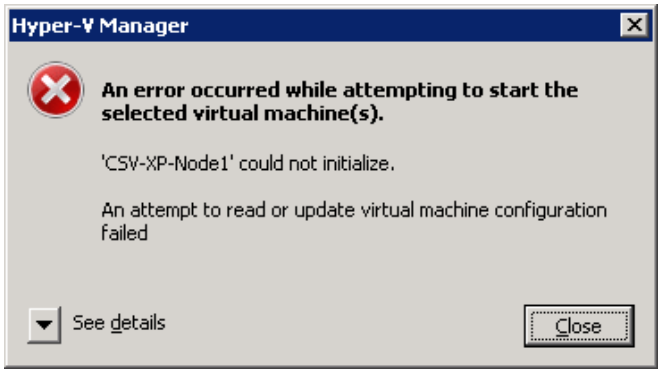
2. Under Virtual Machines, right click on the newly restored virtual machine, select [Setting].

3. For each virtual disk that was not restored, remove the corresponding [Hard Drive] setting from [Hardware].



4. Start the virtual machine afterward.

Important:
If the following error is displayed during the startup, please remove the Saved State of the corresponding VM.


Hyper-V Manager
An error occurred while attempting to start the selected virtual machine(s).
'CSV-XP-Node1' could not initialize.
An attempt to read or update virtual machine configuration failed
See details
Close

In Hyper-V Manager, right click on the corresponding VM and select [Delete Saved State], start the VM again afterward.

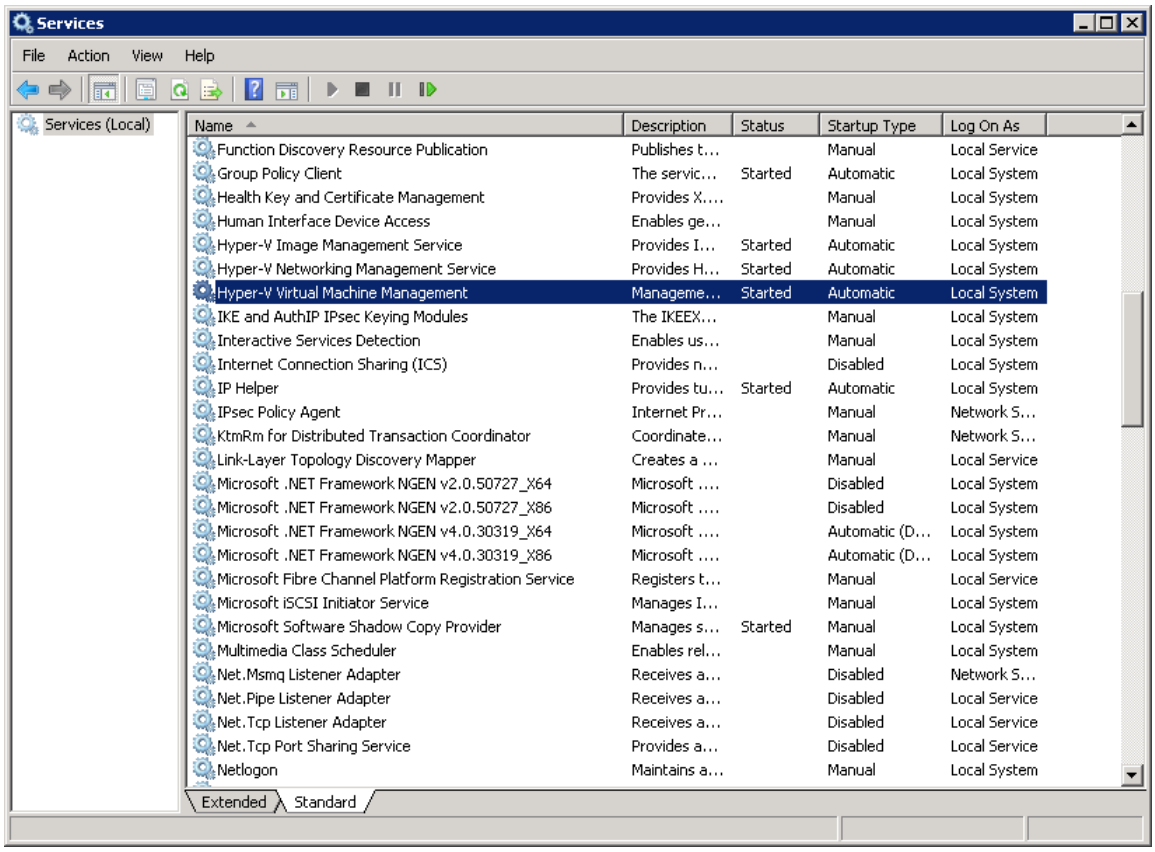
For original virtual machine with snapshot

1. Locate the virtual machine's folder location on the Hyper-V server.

   Important:
   Serious problem may occur if the configuration files are incorrectly modified; it may prevent the virtual machine from starting.

   Please only perform the following procedures if you have in-depth knowledge on Hyper-V.

2. Stop the Hyper-V Virtual Machine Management service.


Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
Function Discovery Resource Publication Publishes t... Manual Local Service
Group Policy Client The servic... Started Automatic Local System
Health Key and Certificate Management Provides X.... Manual Local System
Human Interface Device Access Enables ge... Manual Local System
Hyper-V Image Management Service Provides I... Started Automatic Local System
Hyper-V Networking Management Service Provides H... Started Automatic Local System
Hyper-V Virtual Machine Management Manageme... Started Automatic Local System
IKE and AuthIP IPsec Keying Modules The IKEEX... Manual Local System
Interactive Services Detection Enables us... Manual Local System
Internet Connection Sharing (ICS) Provides n... Disabled Local System
IP Helper Provides tu... Started Automatic Local System
IPsec Policy Agent Internet Pr... Manual Network S...
KtmRm for Distributed Transaction Coordinator Coordinate... Manual Network S...
Link-Layer Topology Discovery Mapper Creates a ... Manual Local Service
Microsoft .NET Framework NGEN v2.0.50727_X64 Microsoft .... Disabled Local System
Microsoft .NET Framework NGEN v2.0.50727_X86 Microsoft .... Disabled Local System
Microsoft .NET Framework NGEN v4.0.30319_X64 Microsoft .... Automatic (D... Local System
Microsoft .NET Framework NGEN v4.0.30319_X86 Microsoft .... Automatic (D... Local System
Microsoft Fibre Channel Platform Registration Service Registers t... Manual Local Service
Microsoft iSCSI Initiator Service Manages I... Manual Local System
Microsoft Software Shadow Copy Provider Manages s... Started Manual Local System
Multimedia Class Scheduler Enables rel... Manual Local System
Net.Msmq Listener Adapter Receives a... Disabled Network S...
Net.Pipe Listener Adapter Receives a... Disabled Local Service
Net.Tcp Listener Adapter Receives a... Disabled Local Service
Net.Tcp Port Sharing Service Provides a... Disabled Local Service
Netlogon Maintains a... Manual Local System
Extended Standard

3. Remove the corresponding entry from the Virtual Machine configuration *${VM-GUID}.xml* file.

   - Open the corresponding *${VM-GUID}.xml* file at the following location with a text editor.

```
${VM-Location}\Virtual Machine\${VM-GUID}.xml
```

   - Locate the line of all non existing VHD.

```
<controller0>
    <drive0>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard Disks\Name_GUID.avhd</pathname>
        <type type="string">VHD</type>
    </drive0>
    <drive1>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard
        Disks\Second_Disk_GUID.avhd</pathname>
        <type type="string">VHD</type>
    </drive1>
</controller0>
```

   - Modify the line from:

     <type type="string">VHD</type>

     To

     <type type="string">NONE</type>

```
<controller0>
    <drive0>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard Disks\Name_GUID.avhd</pathname>
        <type type="string">VHD</type>
    </drive0>
    <drive1>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard
        Disks\Second_Disk_GUID.avhd</pathname>
        <type type="string">NONE</type>
    </drive1>
</controller0>
```

   - Save the changes afterward.

4. Remove the corresponding entry from the Snapshot configuration *${GUID}.xml* file.

   - Open the corresponding snapshot's *${GUID}.xml* file at the following location with a text editor.

```
${VM-Location}\Snapshots\${GUID}.xml
```

   - Locate the line of all non existing virtual disk.

```
<controller0>
    <drive0>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard Disks\Name_GUID.vhd</pathname>
        <type type="string">VHD</type>
    </drive0>
    <drive1>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard
        Disks\Second_Disk_GUID.vhd</pathname>
        <type type="string">VHD</type>
    </drive1>
</controller0>
```

   - Modify the line from:

     <type type="string">VHD</type>

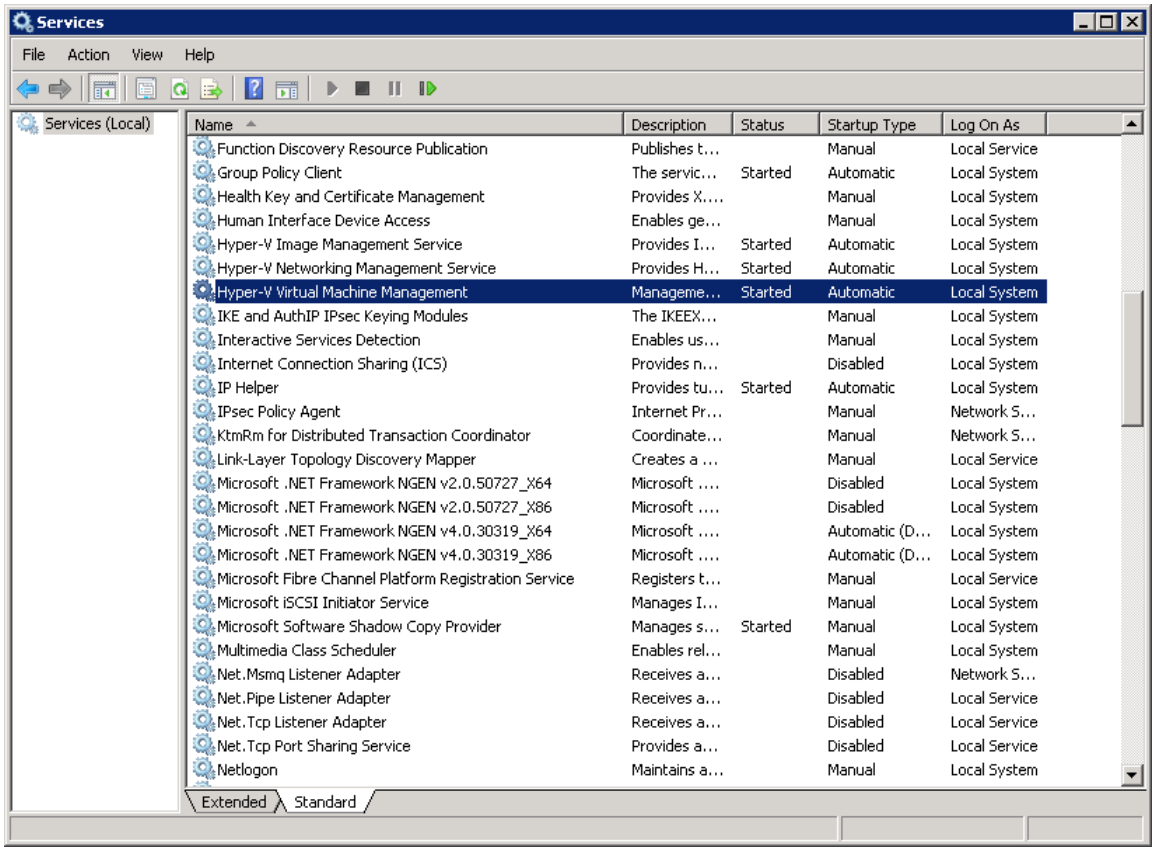
     To

     <type type="string">NONE</type>

```
<controller0>
    <drive0>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard Disks\Name_GUID.vhd</pathname>
        <type type="string">VHD</type>
    </drive0>
    <drive1>
        <pathname type="string">D:\Hyper-V\Virtual Machine
        Name\Virtual Hard
        Disks\Second_Disk_GUID.vhd</pathname>
        <type type="string">NONE</type>
    </drive1>
</controller0>
```

- Repeat the same step for each snapshot.

5. Start the Hyper-V Virtual Machine Management service.

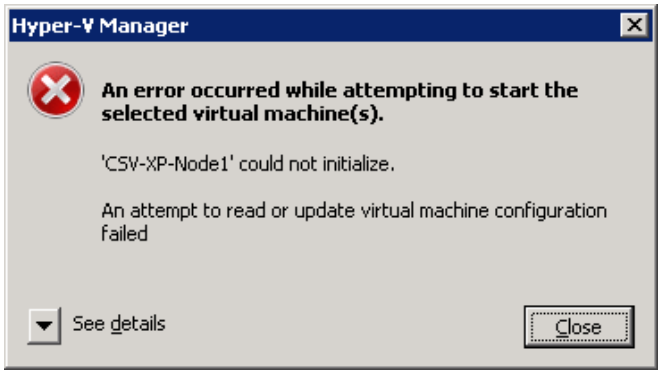

Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
Function Discovery Resource Publication Publishes t... Manual Local Service
Group Policy Client The servic... Started Automatic Local System
Health Key and Certificate Management Provides X.... Manual Local System
Human Interface Device Access Enables ge... Manual Local System
Hyper-V Image Management Service Provides I... Started Automatic Local System
Hyper-V Networking Management Service Provides H... Started Automatic Local System
Hyper-V Virtual Machine Management Manageme... Started Automatic Local System
IKE and AuthIP IPsec Keying Modules The IKEEX... Manual Local System
Interactive Services Detection Enables us... Manual Local System
Internet Connection Sharing (ICS) Provides n... Disabled Local System
IP Helper Provides tu... Started Automatic Local System
IPsec Policy Agent Internet Pr... Manual Network S...
KtmRm for Distributed Transaction Coordinator Coordinate... Manual Network S...
Link-Layer Topology Discovery Mapper Creates a ... Manual Local Service
Microsoft .NET Framework NGEN v2.0.50727_X64 Microsoft .... Disabled Local System
Microsoft .NET Framework NGEN v2.0.50727_X86 Microsoft .... Disabled Local System
Microsoft .NET Framework NGEN v4.0.30319_X64 Microsoft .... Automatic (D... Local System
Microsoft .NET Framework NGEN v4.0.30319_X86 Microsoft .... Automatic (D... Local System
Microsoft Fibre Channel Platform Registration Service Registers t... Manual Local Service
Microsoft iSCSI Initiator Service Manages I... Manual Local System
Microsoft Software Shadow Copy Provider Manages s... Started Manual Local System
Multimedia Class Scheduler Enables rel... Manual Local System
Net.Msmq Listener Adapter Receives a... Disabled Network S...
Net.Pipe Listener Adapter Receives a... Disabled Local Service
Net.Tcp Listener Adapter Receives a... Disabled Local Service
Net.Tcp Port Sharing Service Provides a... Disabled Local Service
Netlogon Maintains a... Manual Local System
Extended Standard

6. Remove any existing snapshot.

Important:
The restored virtual machine does not support the reversion of previous snapshots if they contain virtual disks not restored.

7. Start the virtual machine.

Important:
If the following error is displayed during the startup, please remove the Saved State of the corresponding VM.


Hyper-V Manager
An error occurred while attempting to start the selected virtual machine(s).
'CSV-XP-Node1' could not initialize.
An attempt to read or update virtual machine configuration failed
See details
Close

In Hyper-V Manager, right click on the corresponding VM and select [Delete Saved State], start the VM again afterward.

14.2.7 How to restore individual virtual disk of Microsoft virtual machines in cluster environment

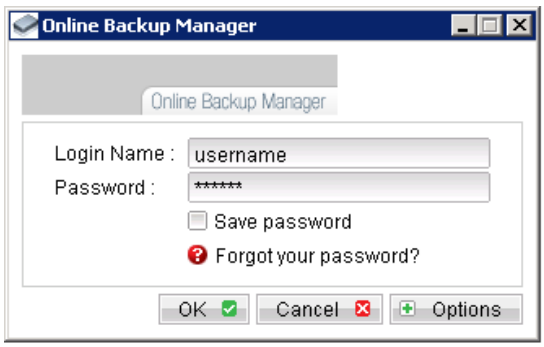
Individual virtual disk can be restored to the original VM, or to be added to a new VM.

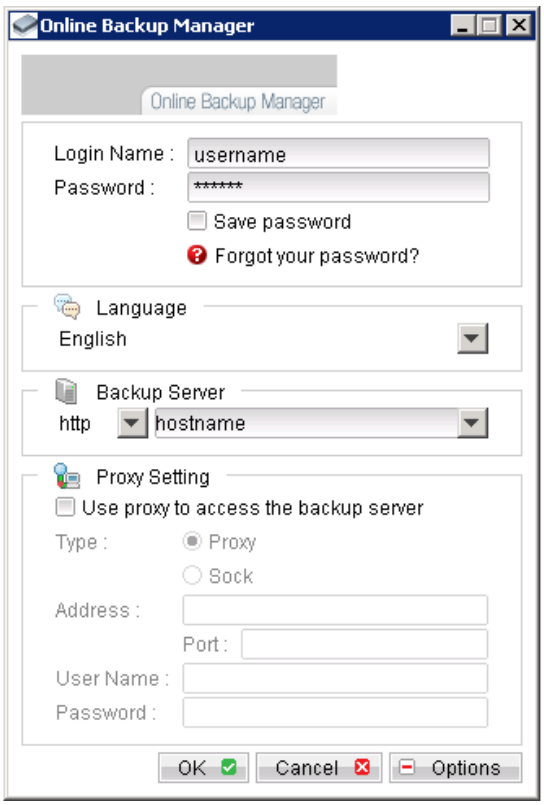
Important:
Serious problem may occur if the configuration files are incorrectly modified; it may prevent the virtual machine from starting.

Please only perform the following procedures if you have in-depth knowledge on Hyper-V.

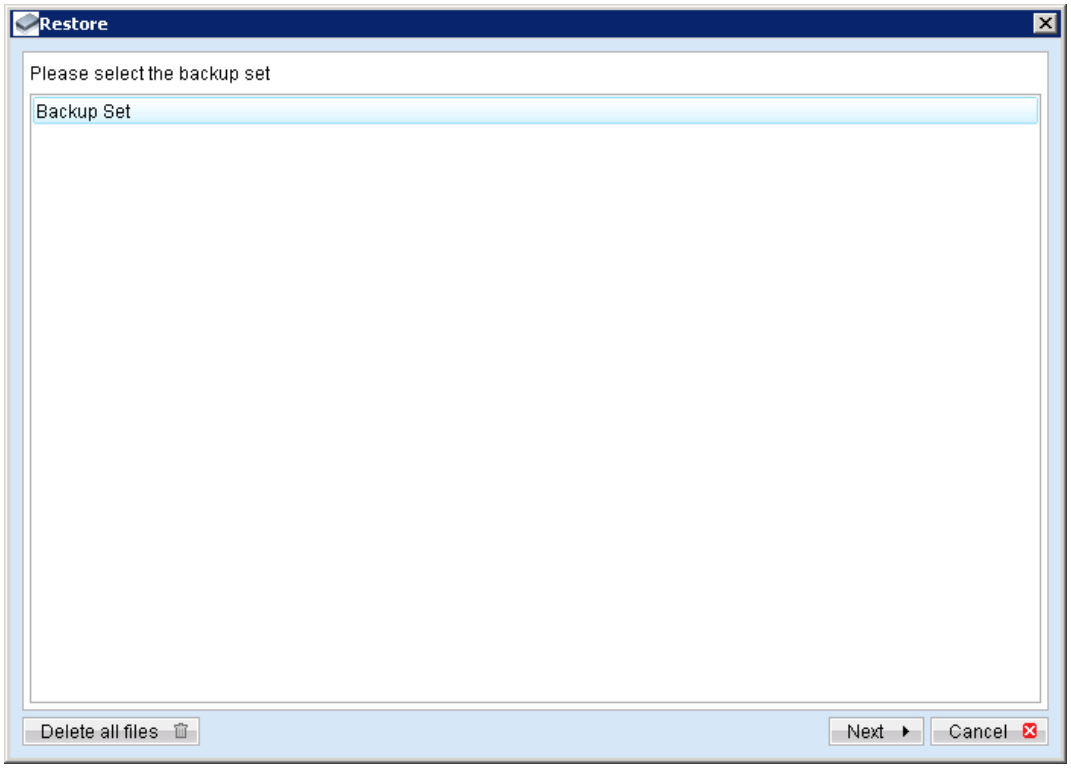
14.2.1.7 How to restore individual virtual disk to the original VM

1. Open Hyper-V Manager.
2. Shutdown the VM to be restored to.
3. Login to the backup application's user interface.



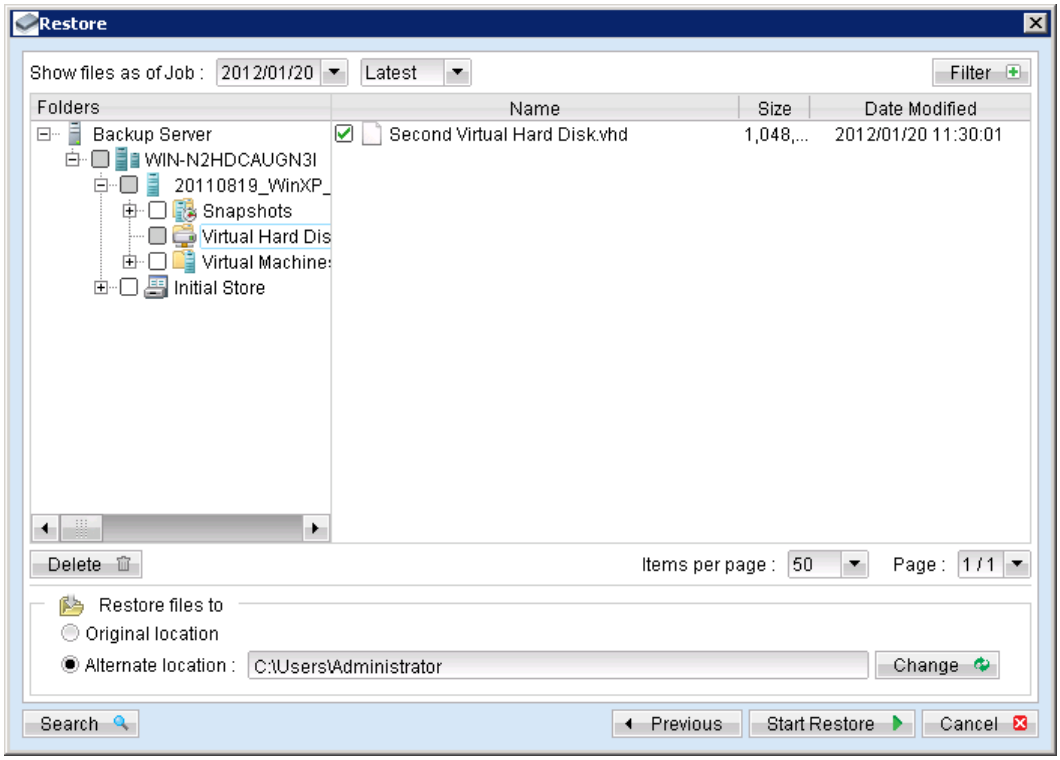


4. Select the [Restore] button and the corresponding backup set.



5. Select [Alternate location], then select the virtual disk to be restored.

   Restore of individual virtual disk is only supported for restore to [Alternation location].

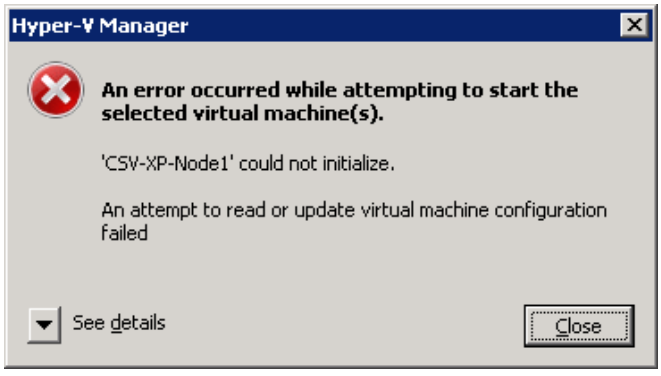


6. Click [Change]; select the directory path where the virtual disk was originally backed up from.

7. Click the [Start Restore] button to begin the restore process.

8. Start the virtual machine after the restore process is completed.

Important:
If the following error is displayed during the startup, please remove the Saved State of the corresponding VM.

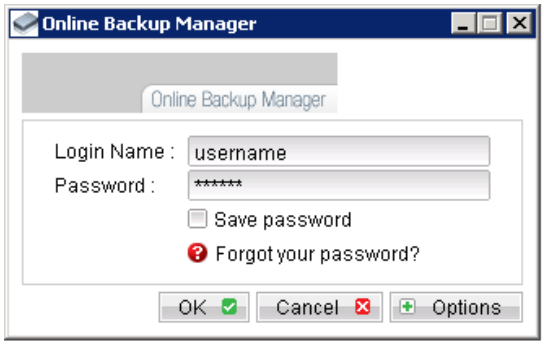

Hyper-V Manager
An error occurred while attempting to start the selected virtual machine(s).
'CSV-XP-Node1' could not initialize.
An attempt to read or update virtual machine configuration failed
See details
Close

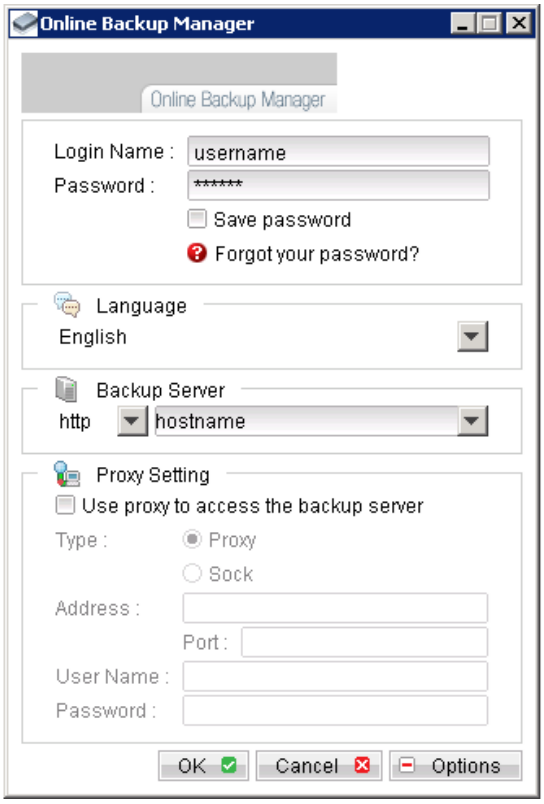
In Hyper-V Manager, right click on the corresponding VM and select [Delete Saved State], start the VM again afterward.

14.2.2.7 How to restore individual virtual disk to a different VM

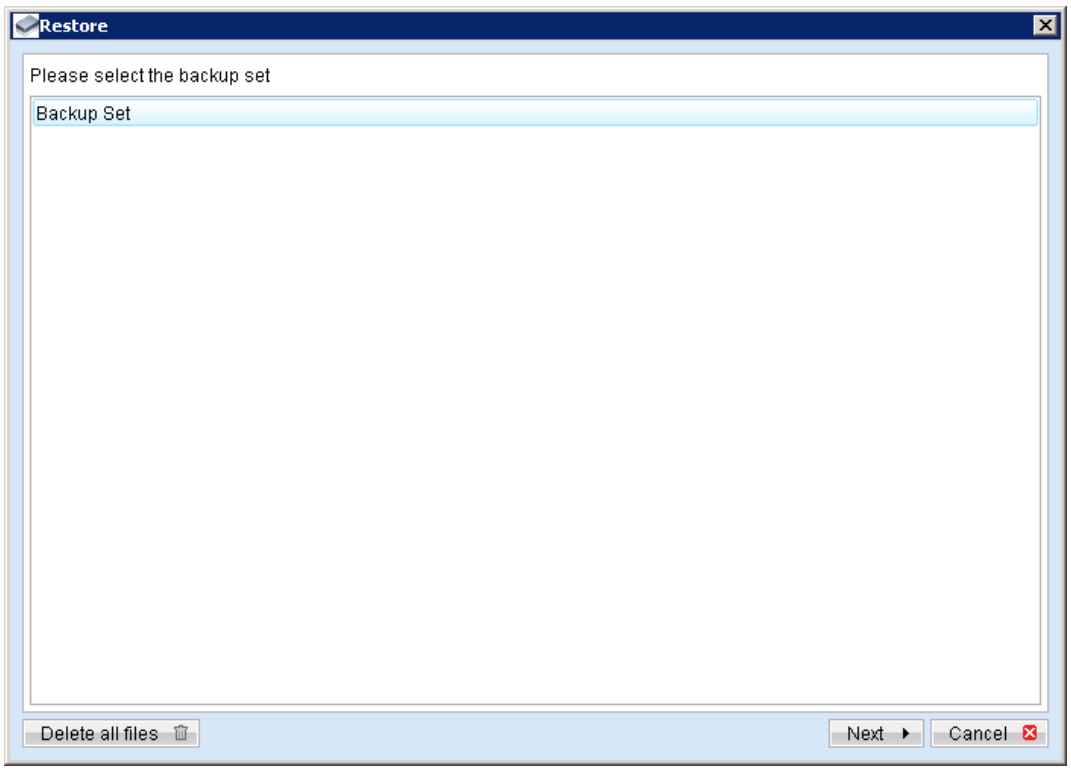
Important:
Restore of individual virtual disk to a different virtual machine is only supported for virtual disk with no snapshot.

1. Login to the backup application's user interface.



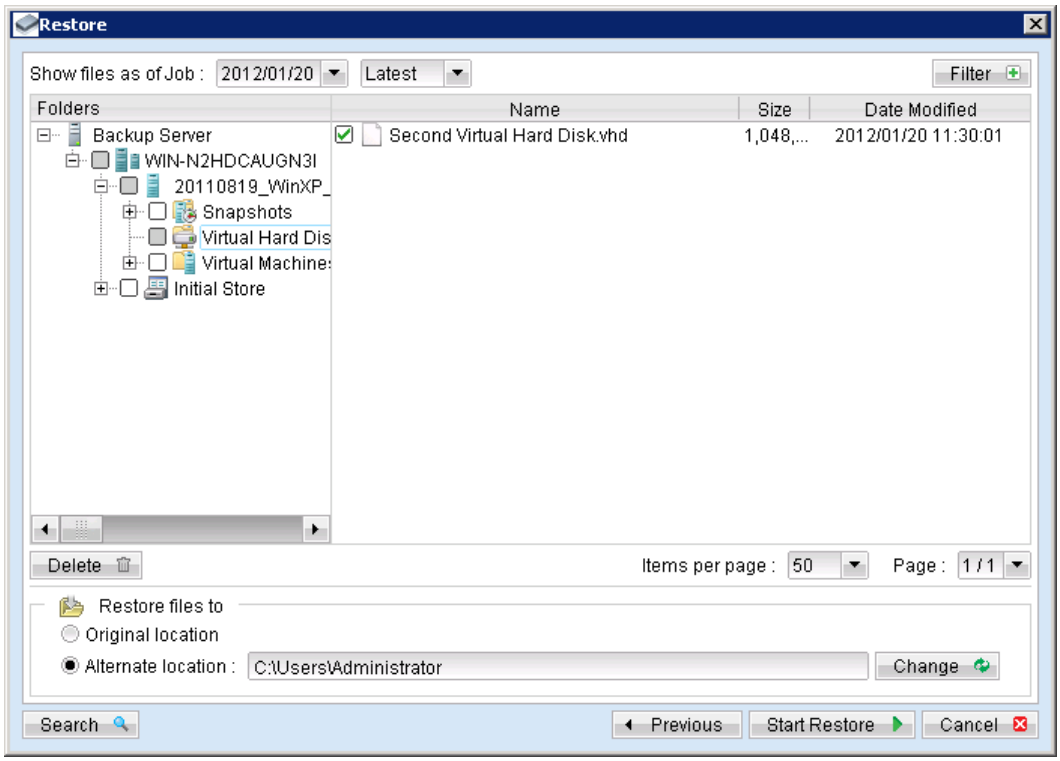


2. Select the [Restore] button and the corresponding backup set.



3. Select [Alternate location], then select the virtual disk to be restored.

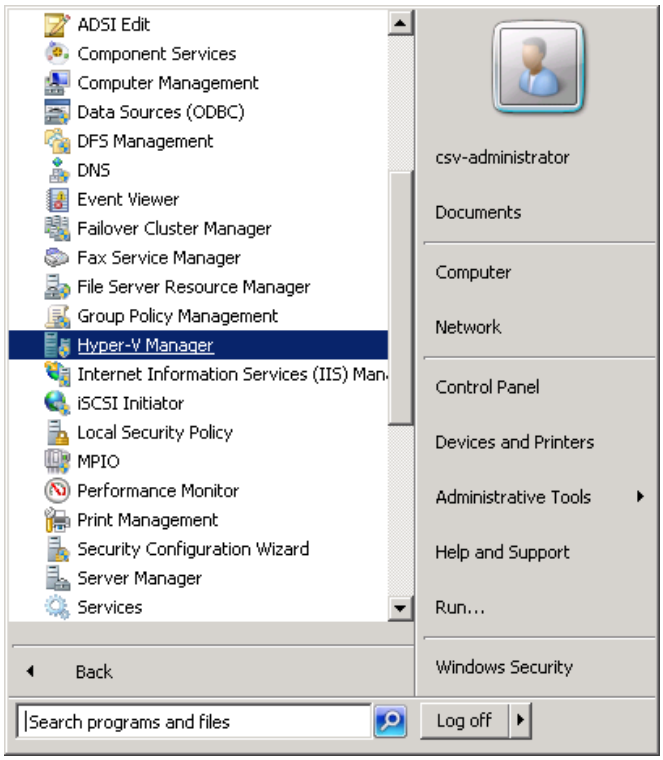
   Restore of individual virtual disk is only supported for restore to [Alternation location].



4. Click [Change] to select the location where the virtual disk should be restored.

5. Click the [Start Restore] button to begin the restore process.

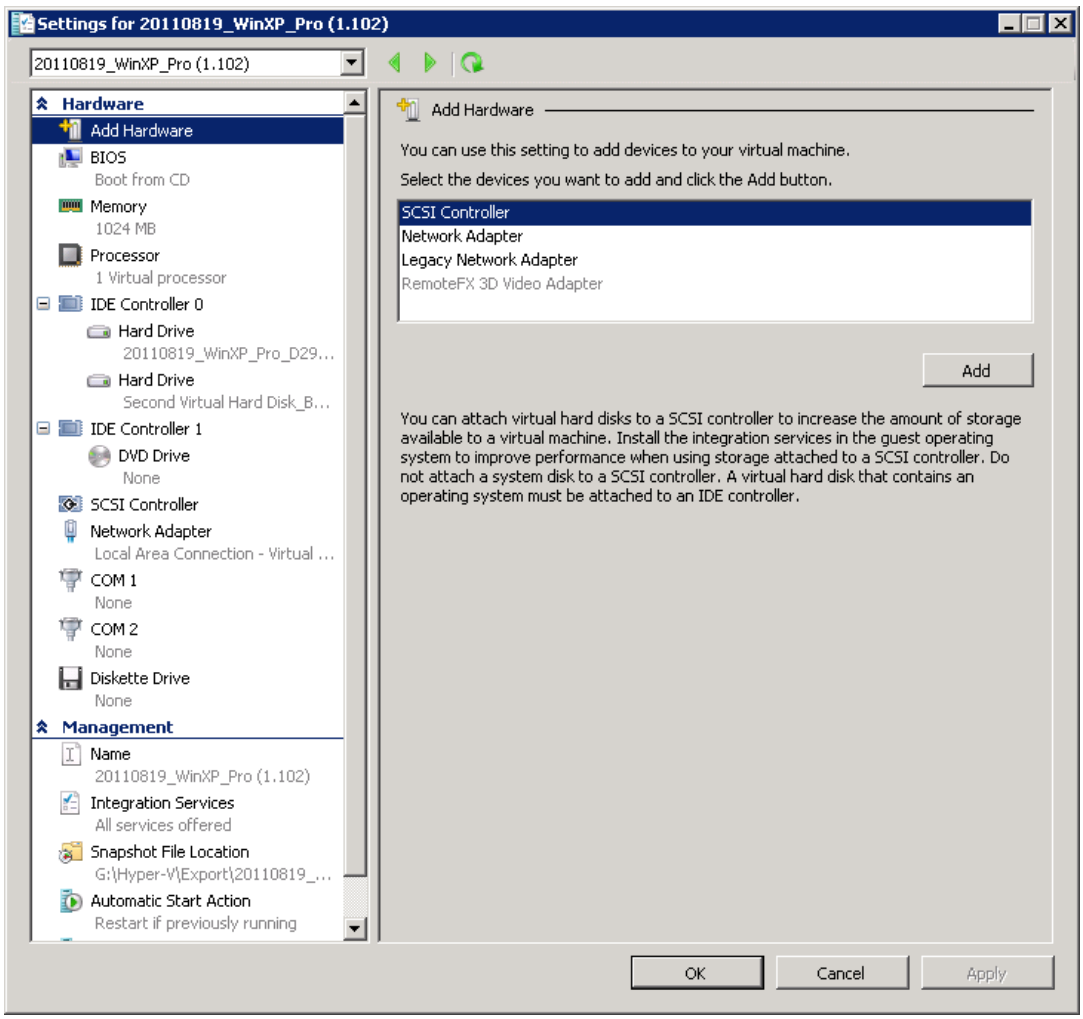
6. When the restore process is completed, open Hyper-V Manager.



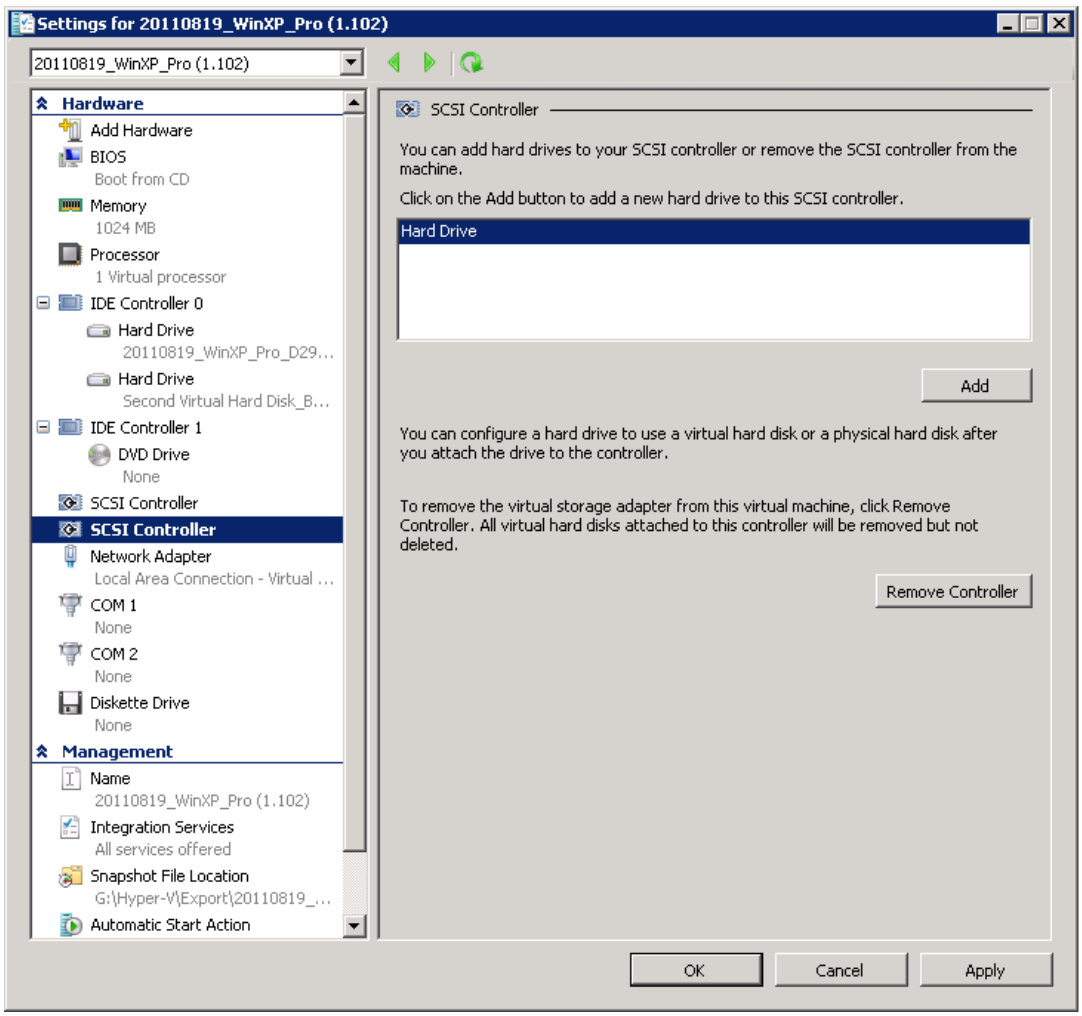
7. Under Virtual Machines, powers down the corresponding virtual machine to be restored to.

8. Select [Setting] to add the restored virtual disk to the VM.

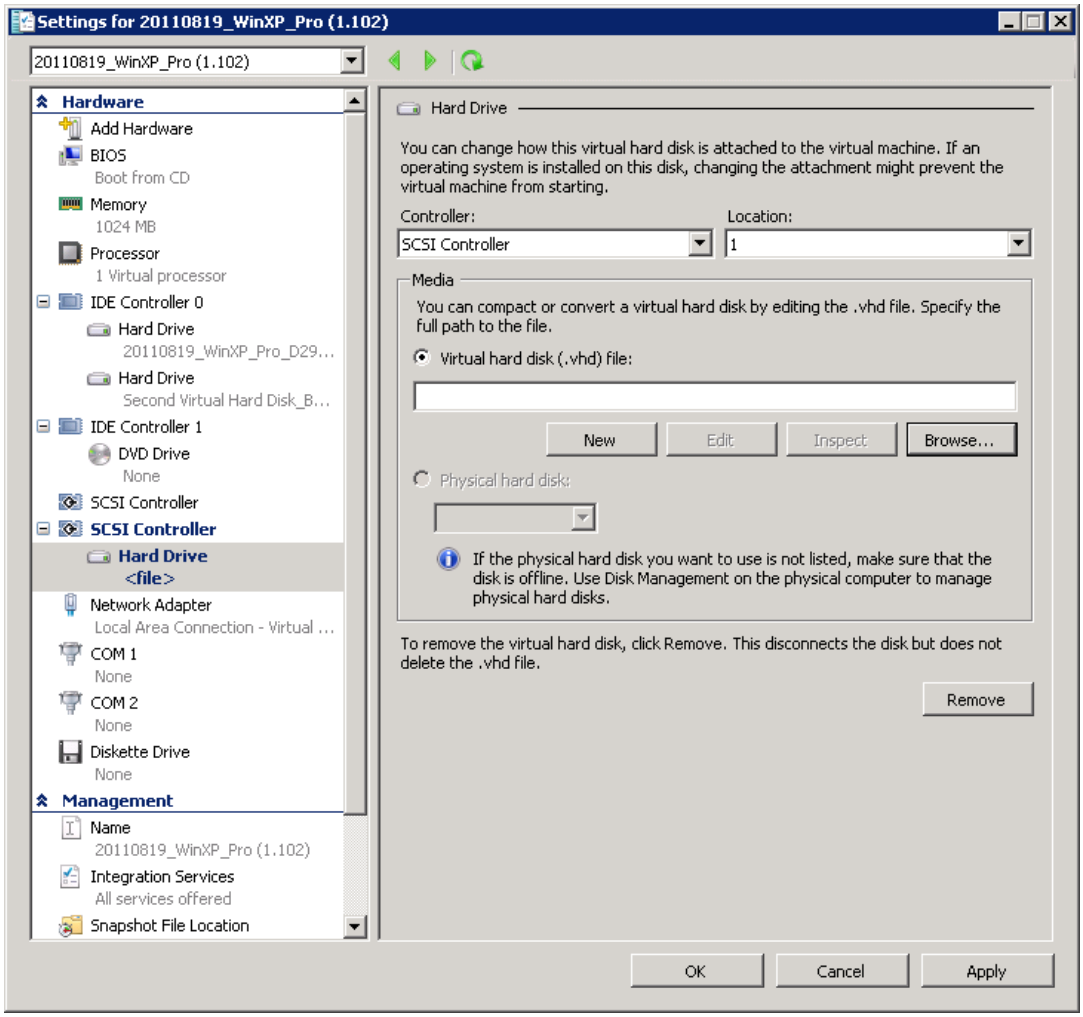
9. Select [Add Hardware], [SCSI Controller] and press the [Add] button.



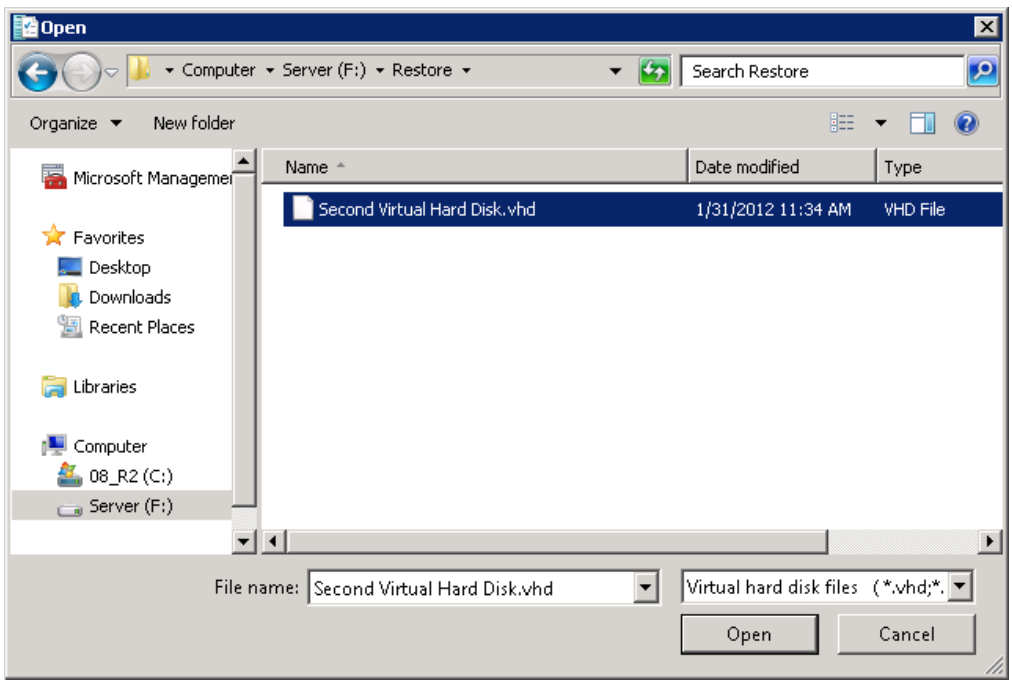
10. Select [Hard Drive] and press the [Add] button.



11. Select the corresponding [Controller] and [Location] setting.



12. Under Media, select [Browse] and browse to the newly restored virtual disk file.



13. Start the virtual machine.

15 Backup / Restore Microsoft Exchange Server

This chapter describes in details how to backup and restore Microsoft Exchange Server with OBM.

15.1 Supported versions

The MS Exchange Server backup module is supported for the following Exchange versions:

- MS Exchange 2003
- MS Exchange 2007
- MS Exchange 2010 / SP1

For more details, please refer to Help Centre Article:
https://help..com/openArticle.aspx?aid=2323

15.2 Backup Microsoft Exchange Server 2003 / 2007

15.2.1 Requirements and recommendations

Please ensure that the following requirements are met by the MS Exchange server:

1. OBM is installed on the MS Exchange server.

2. The Exchange databases selected for backup will be temporarily spooled to a temp directory before being uploaded to the backup server.

   It is recommended that the temporary directory have disk space of at least 120% of the total database size (e.g. total size of all .edb files found within the MS Exchange Server installation folder).

3. It is recommended that the temporary directory be configured on a local drive.

4. For Exchange server with Active Directory installed, a System State backup must be performed regularly with the MS Exchange server backup.

15.2.2 Overview

For a complete Exchange server backup, backup for the following components must be performed:

System State

For Exchange server with Active Directory installed, as part of the restore, the system state of the server must also be restored.

Running regular system state backups of the Exchange is therefore crucial, as it ensures that the system state data is synchronized with the Exchange database data.

Information Store (Exchange 2003 / 2007)
The Information Store of Exchange 2003 and 2007 contains both mailbox store and public folder store data.

The server stores data into two files - *.edb* and *.stm* file that forms an Exchange store repository.

The default mailbox store on an Exchange 2003 server uses filename *Priv1.edb* and *Priv1.stm*; the default public folder store uses the filename *Pub1.edb* and *Pub1.stm*.

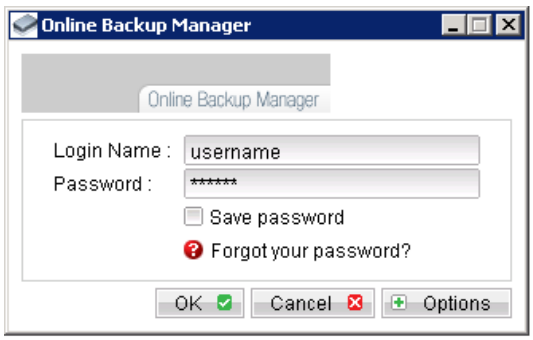
The *.edb* file contains tables that hold metadata for all e-mail messages and other items in the Exchange store, while *.stm* stores native Internet content.

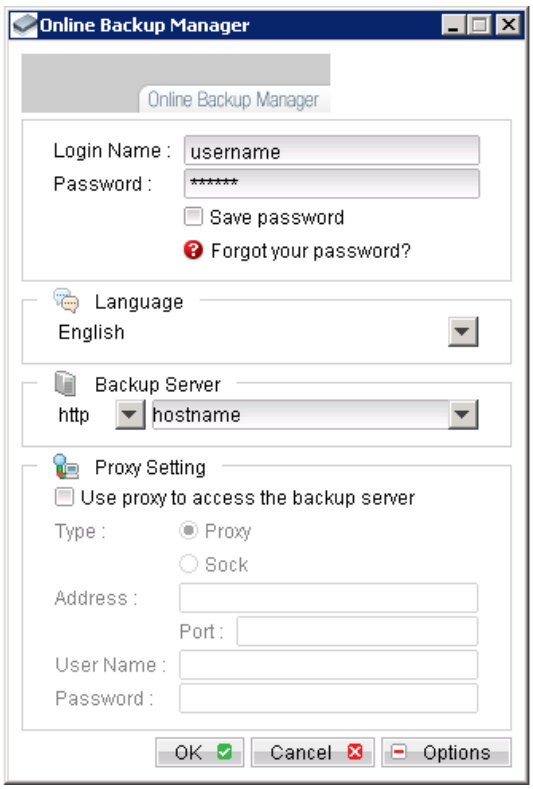
15.2.3 How to backup Microsoft Exchange Server 2003 / 2007

Refer to the following instructions to backup Microsoft Exchange Server 2003 or 2007:

1. Install OBM on the MS Exchange Server.

2. Login to the backup application's user interface.



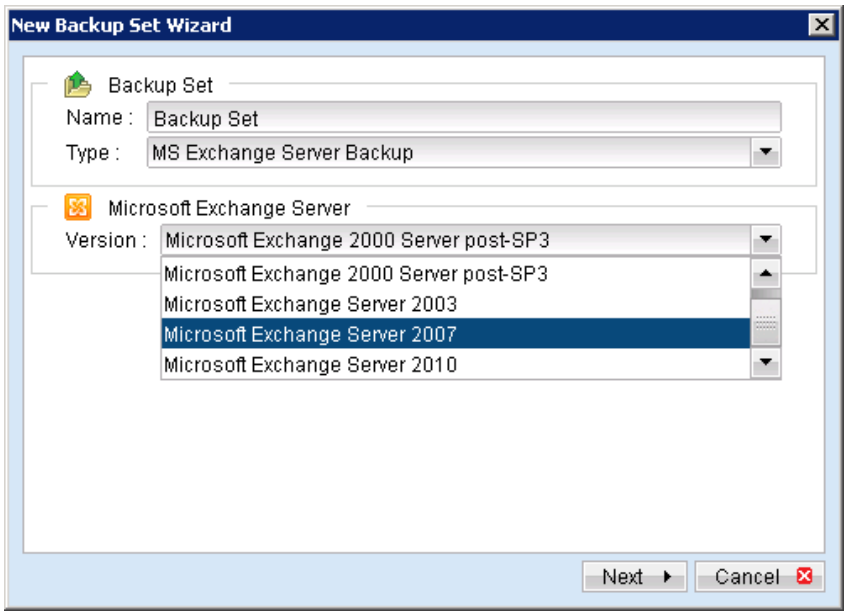


3. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

4. Enter the name of the backup set.

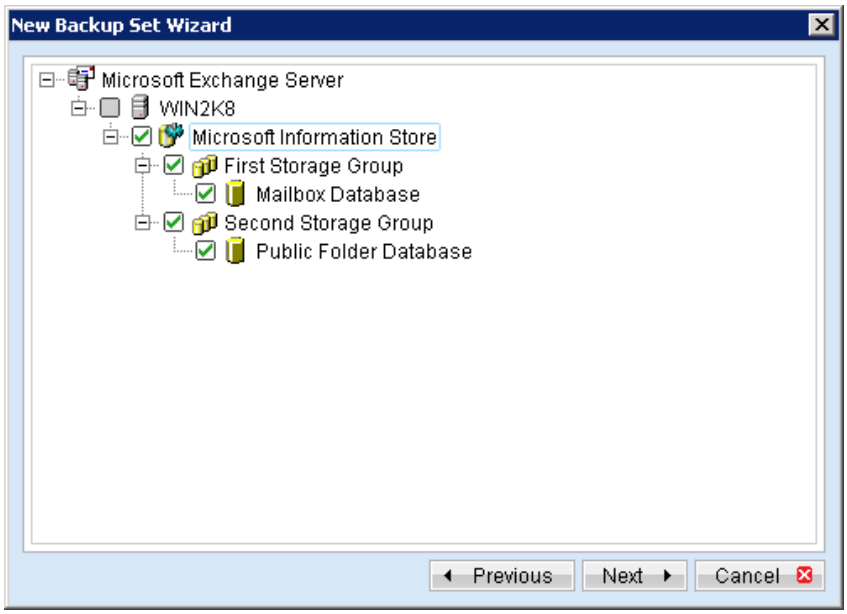
5. Create a MS Exchange Server Backup set by selecting [MS Exchange Server Backup] from the backup set type dropdown menu.

6. Select the corresponding Exchange version from the version dropdown menu.

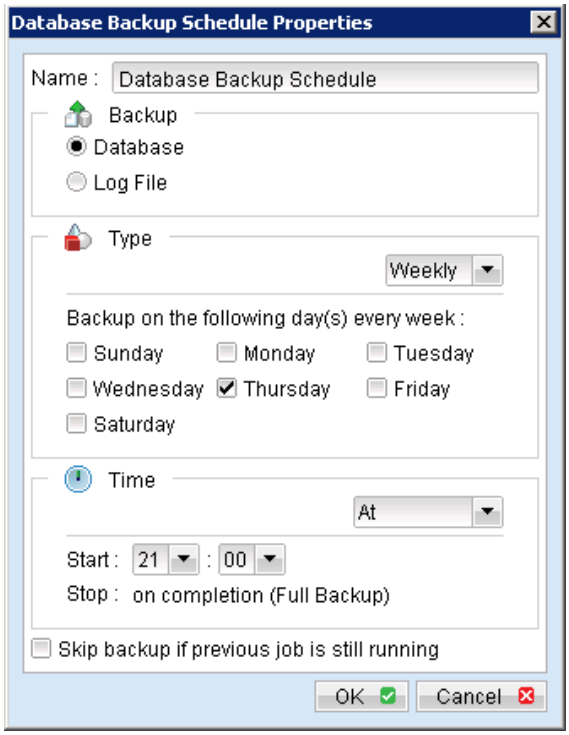


7. Select [Next] to proceed.

8. In the backup source selection screen, select the Information Store for backup.



9. Configure a backup schedule for unattended backups.



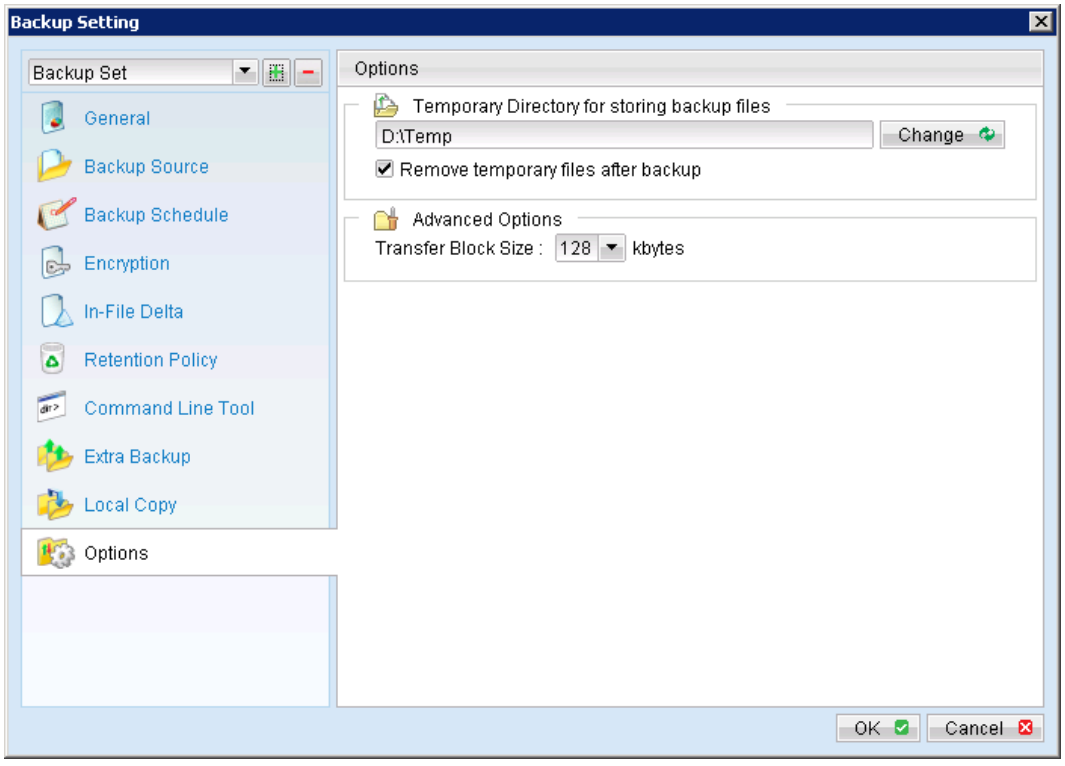
Menu Items	Description
Name	Enter a backup schedule name of your choice.
Backup	Select backup type [Database / Log File].

	Note: Select database type for full database backup, or select log file type for transaction log backup.
Type	Select backup schedule type [Daily / Weekly / Monthly / Custom].
Time	Select backup schedule time type [At / Periodically]. Note: Select backup schedule time at to perform backup at a certain time, or select backup schedule time periodically to perform backup every X minutes / hours.
Skip backup if previous job is still running	Select whether to stop the backup job from running if a previous backup job is still running.

10. Select an encryption setting for your backup set.

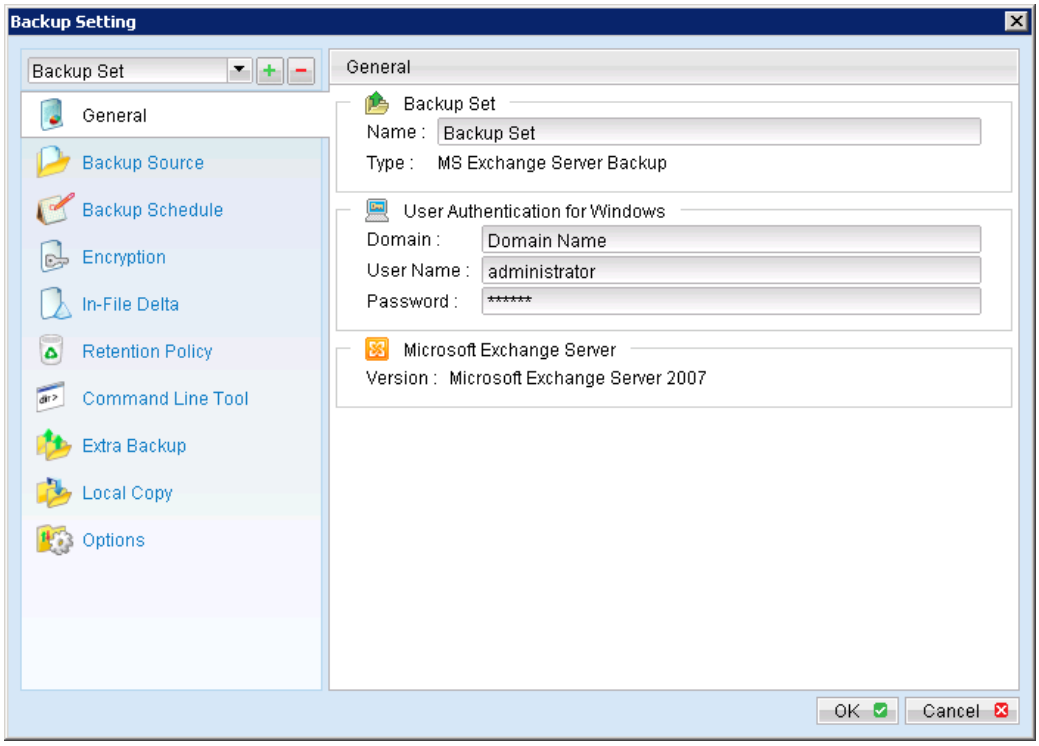
11. Press the [OK] button to complete the configuration of the [New Backup Size Wizard].

12. Configure the temporary backup folder, select [Backup Setting], [Options].

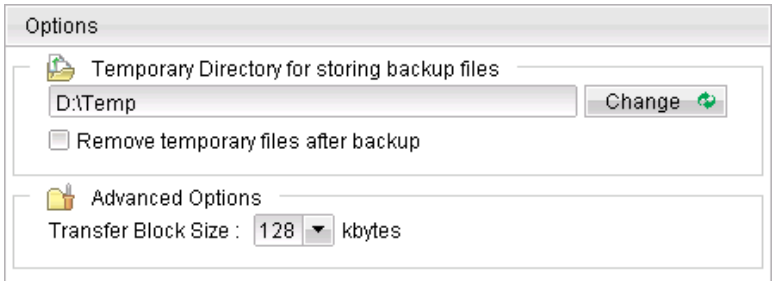


Note:
The temporary directory can be set to a local or network path.

Please be reminded to fill in the [User Authentication for Windows] setting if a network path is selected.

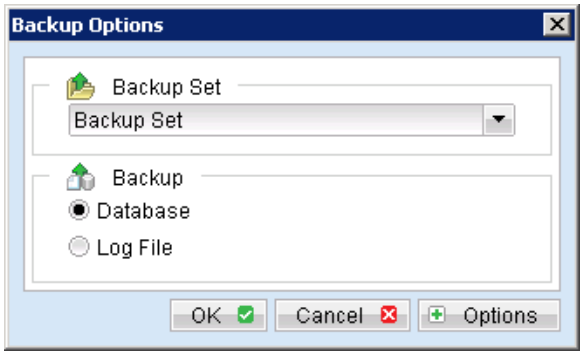


For database specific backup type, data files spooled by the **latest backup job** can be kept by disabling the [Remove temporary files after backup] option.



13. Scheduled backup will run automatically at the configured schedule time.

14. Click [Backup] button on the left panel to perform a backup immediately.



Menu Items	Description
Backup	Select backup type [Database / Log File]. Note: Select [Database] type for full database backup, or select [Log File] type for transaction log backup.

Important:
For Exchange server with Active Directory installed, a System State backup must be performed regularly with the MS Exchange server backup.

15.3 Restore Microsoft Exchange Server 2003 / 2007

Refer to the following instructions to restore Microsoft Exchange Server 2003 / 2007:

1. Prepare the operating system for the Exchange Server restore (if required).

   Install the original version of Windows and Exchange Server (with the same level of service pack installed as in the original system).

2. Restore Windows Active Directory (if required).

   Restore the System State data from OBS, and then restore the System State using Ntbackup / WBAdmin.exe.

   Refer to the "How to restore Windows System State" chapter for detailed instruction.

3. Install OBM (if required).

   Refer to the Installing OBM chapter for details instruction.

4. Startup the [Microsoft Information Store] services from Windows Services.

5. Restore the Exchange database from backup; restore the database backup files from the OBS server.

   Please ensure the directory structure is the same as it appears in the File Explorer:

```
-->[Restore Destination]
------>[Server]
---------->[Microsoft Information Store]
-------------->[First Storage Group]
------------------>[Mailbox Store(Server)]
---------------------->Priv1.edb
---------------------->Priv1.stm
------------------>[Public Folder Store(Server)]
---------------------->Pub1.edb
---------------------->Pub1.stm
---------------------->E0000001.log
```

   If a different version of the database to be restored exists on the MS Exchange server, please dismount it from the services using System Manager or Exchange Management Console for MS Exchange 2003 and 2007 respectively.

6. Use the [ExchangeRestore32.exe / ExchangeRestore64.exe] file found from the OBM [bin] directory to restore the database.

   For 32bit MS Exchange installation:
   ${OBM-Install-Home}\bin\ExchangeRestore32.exe

   For 64bit MS Exchange installation:
   ${OBM-Install-Home}\bin\ExchangeRestore64.exe

   Example 1
   For restore of all databases from backup data [E:\Backup] to an Exchange Server named [win2k8] using the temporary directory [E:\Temp]

   Backup data source = E:\Backup
   Temp folder for restore process = E:\Temp
   Exchange server name = Win2k8

   The following command can be used:

Exchange server recovery - Example 1

```
C:\Program Files\OBM\bin>ExchangeRestore64 DIR="E:\Backup"
TEMP="E:\Temp" SERVER="win2k8"

Microsoft Exchange Server 2000/2003/2007 Backup Recovery
Utility

 [Start] Exchange Server - 'win2k8'
  [Start] Service - 'Microsoft Information Store'
   [Start] Storage Group - 'First Storage Group'
    [Start] Database - 'Mailbox Database'
     Restoring file 'C:\Program Files\Microsoft\Exchange
Server\Mailbox\First Storage Group\Mailbox
Database.edb' ...
    [End] Database - 'Mailbox Database'
    [Start] Restoring transaction log - 'First Storage
Group'
     Restoring Log File 'E:\Temp\restore.tmp\First Storage
Group\E000000B7CF.log' ...
     Restoring Log File 'E:\Temp\restore.tmp\First Storage
Group\E000000B7D0.log' ...
     Restoring Log File 'E:\Temp\restore.tmp\First Storage
Group\E000000B7D1.log' ...
    [End] Restoring transaction log - 'First Storage
Group'
    [Start] Applying transaction log ...
    [End] Applying transaction log
   [End] Storage Group - 'First Storage Group'
   [Start] Storage Group - 'Second Storage Group'
    [Start] Database - 'Public Folder Database'
     Restoring file 'C:\Program Files\Microsoft\Exchange
Server\Mailbox\Second Storage Group\Public Folder
```

```
Database.edb' ...
    [End] Database - 'Public Folder Database'
    [Start] Restoring transaction log - 'Second Storage
Group'
     Restoring Log File 'E:\Temp\restore.tmp\Second
Storage Group\E0100004F10.log' ...
     Restoring Log File 'E:\Temp\restore.tmp\Second
Storage Group\E0100004F11.log' ...
    [End] Restoring transaction log - 'Second Storage
Group'
    [Start] Applying transaction log ...
    [End] Applying transaction log
   [End] Storage Group - 'Second Storage Group'
  [End] Service - 'Microsoft Information Store'
 [End] Exchange Server - 'win2k8'
```

Mount the Exchange database afterward in System Manager for Exchange 2003 or Exchange Management Console for Exchange 2007.

Example 2

For restore of database name [mail] in storage group [SG5] from backup data [E:\Backup] to an Exchange Server named [win2k8] using the temporary directory [E:\Temp]

Backup data source = E:\Backup
Temp folder for restore process = E:\Temp
Exchange server name = win2k8
Database to be restored = [Mailbox Database] of storage group [First Storage Group]

The following command can be used:

Exchange server recovery - Example 2

```
C:\Program Files\OBM\bin>ExchangeRestore64 DIR="E:\Backup"
TEMP="E:\Temp" SERVER="win2k8" SERVICE="Microsoft
Information Store" STORAGE="First Storage Group"
DATABASE="Mailbox Database"

Microsoft Exchange Server 2000/2003/2007 Backup Recovery
Utility

    [Start] Database - 'Mailbox Database'
     Restoring file 'C:\Program Files\Microsoft\Exchange
Server\Mailbox\First Storage Group\Mailbox
Database.edb' ...
    [End] Database - 'Mailbox Database'
    [Start] Restoring transaction log - 'First Storage
Group'
     Restoring Log File 'E:\Temp\restore.tmp\First Storage
Group\E000000B7CF.log
' ...
```

```
     Restoring Log File 'E:\Temp\restore.tmp\First Storage
Group\E000000B7D0.log
' ...
     Restoring Log File 'E:\Temp\restore.tmp\First Storage
Group\E000000B7D1.log
' ...
    [End] Restoring transaction log - 'First Storage
Group'
    [Start] Applying transaction log ...
    [End] Applying transaction log
```

Mount the Exchange database afterward in System Manager (for Exchange 2003) or Exchange Management Console (for Exchange 2007).

7. Repeat the same procedure for each database to be restored.

   Note:
   Verify under the Event Viewer if there is any error generated during the restore process.

8. If the restore process failed with errors such as bad signature, or null error, the backed up database file restored may be incorrect.

   Please try to manually restore and mount the database and log files.

Mounting database file manually

9. Dismount the Exchange database using the System Manager for Exchange 2003, or Exchange Management Console for Exchange 2007.

10. Copy all restored database and log files to the Exchange database folders.

    Exchange 2003 default folder path is
    ${Exchange-Install-Home}\MDBDATA

    Exchange 2007 default folder path is
    ${Exchange-Install-Home}\Mailbox\First Storage Group
    ${Exchange-Install-Home}\Mailbox\Second Storage Group
    ...

11. Initiate soft recovery mode by applying the transaction log file E00 to the database.

    Enter the following commands:

```
C:\Program Files\Microsoft\Exchange Server\Mailbox\First
Storage Group>eseutil /r e00

Extensible Storage Engine Utilities for Microsoft(R)
```

```
Exchange Server
Version 08.01
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating RECOVERY mode...
    Logfile base name: e00
            Log files: <current directory>
         System files: <current directory>

Performing soft recovery...

Operation completed successfully in 0.813 seconds.
```

12. Repair the database files by running the following commands:

```
C:\Program Files\Microsoft\Exchange Server\Mailbox\First
Storage Group>eseutil /p "Mailbox Database.edb"

Extensible Storage Engine Utilities for Microsoft(R)
Exchange Server
Version 08.01
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating REPAIR mode...
        Database: Mailbox Database.edb
  Temp. Database: TEMPREPAIR3760.EDB

Checking database integrity.

                    Scanning Status (% complete)

          0    10   20   30   40   50   60   70   80   90
100
          |----|----|----|----|----|----|----|----|----|--
--|
          ..................................................
...
```

13. Mount the Exchange database afterward in System Manager for Exchange 2003 or Exchange Management Console for Exchange 2007.

14. The restore of Exchange Server is now completed.

15.4 Backup Microsoft Exchange Server 2010

15.4.1 Requirements and recommendations

Please ensure that the following requirements are met by the MS Exchange server:

1. OBM version 5.5.8.0 or above is installed on the Exchange server.

2. Databases of the Exchange server are spooled to a temporary directory before being uploaded to the offsite backup server.

   It is recommended that the temporary directory have disk space of at least 120% of the total database size (e.g. total size of all .edb files found within the MS Exchange Server installation folder).

3. It is recommended that the temporary directory be configured on a local drive.

4. For Exchange server with Active Directory installed, a System State backup must be performed regularly with the MS Exchange server backup.

5. Backup of Exchange 2010 server in Database Availability Group (DAG) is not supported.

15.4.2 Overview

For a complete Exchange server backup, backup for the following components must be performed:

Windows System State
For Exchange server with Active Directory installed, as part of the restore, the system state must also be restored.

Running regular system state backups of the Exchange is therefore crucial, as it ensures that the system state data is synchronized with the Exchange database data.

Microsoft Information Store (Exchange 2010)
The Information Store of Exchange 2010 contains the data, data definitions, indexes, checksums, flags, and other information that comprise mailboxes in Exchange.

Mailbox databases hold data that's private to an individual user and contain mailbox folders generated when a mailbox is created for that user. A mailbox database is stored as an Exchange database .edb file.

Public folder databases contain the data, their definitions, indexes, checksums, flags, and other information that comprise any public folders in your Exchange organization.

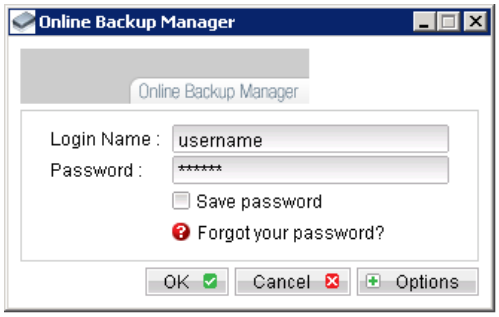
In Exchange Server 2010, public folders are an optional feature.

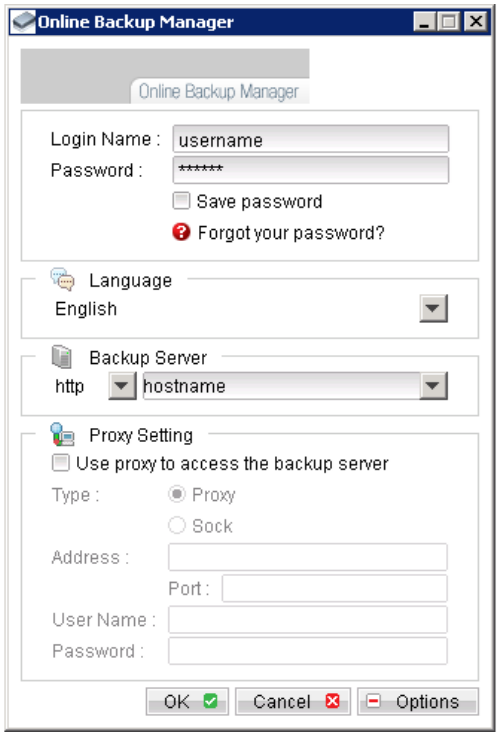
15.4.3 How to backup Microsoft Exchange Server 2010

Refer to follow the instructions to backup Microsoft Exchange Server 2010:

1. Install OBM on the MS Exchange Server.

2. Login to the backup application's user interface.



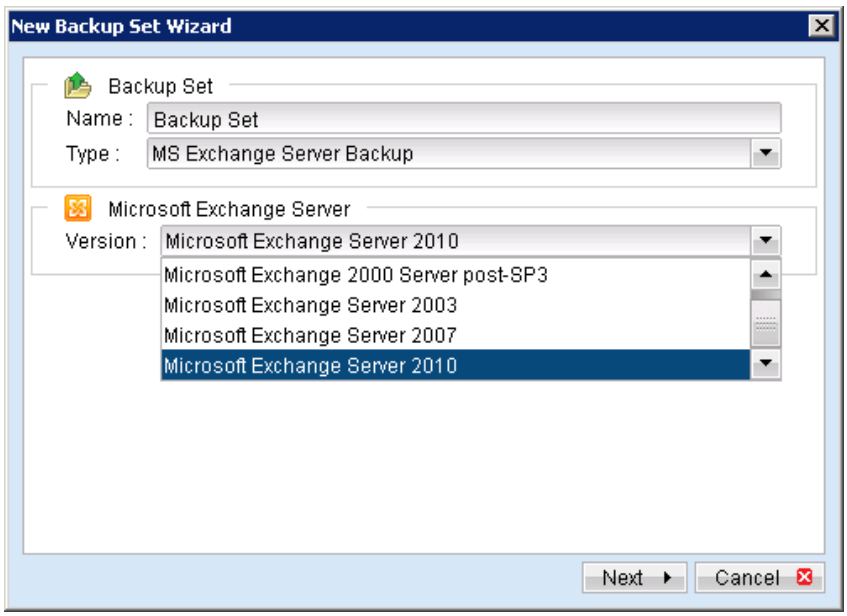


3. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

4. Enter the name of the backup set.

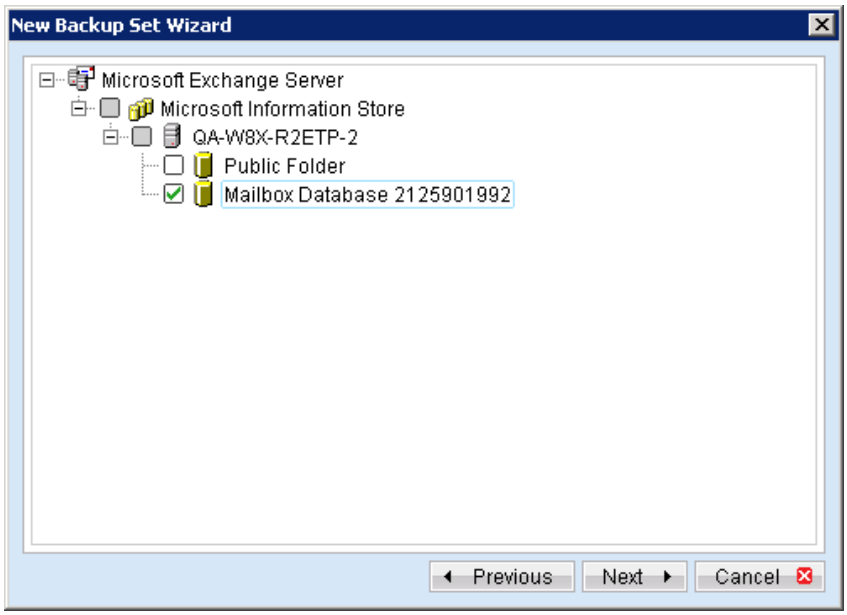
5. Create a MS Exchange Server Backup set by selecting [MS Exchange Server Backup] from the backup set type dropdown menu.

6. Select the corresponding Exchange version from the version dropdown menu.

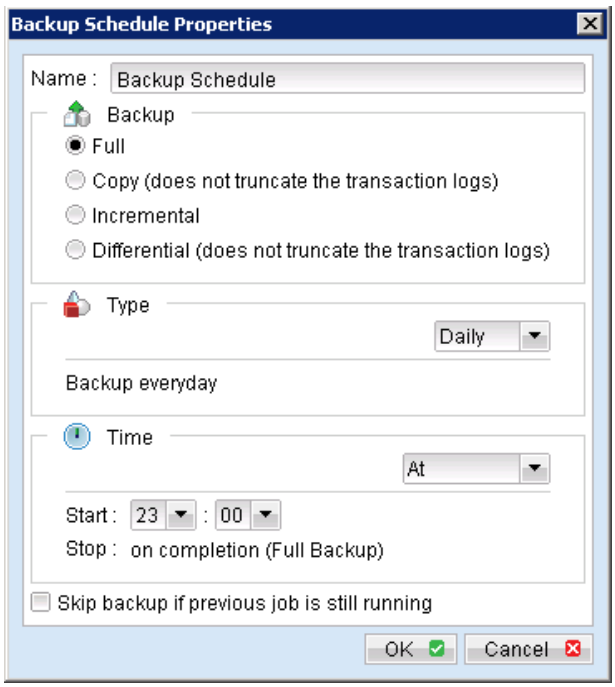


7. Select [Next] to proceed.

8. In the backup source selection screen, select the Information Store for backup.



9. Configure a backup schedule for unattended backups.



Menu Items	Description
Name	Enter a backup schedule name of your choice.
Backup	Select backup type [Full / Copy / Incremental / Differential].
Type	Select backup schedule type [Daily / Weekly / Monthly / Custom].
Time	Select backup schedule time type [At / Periodically]. Note: Select backup schedule time at to perform backup at a certain time, or select backup schedule time periodically to perform backup every X minutes / hours.
Skip backup if pervious job is still running	Select whether to stop the backup job from running if a previous backup job is still running.

Further details on Backup Type:

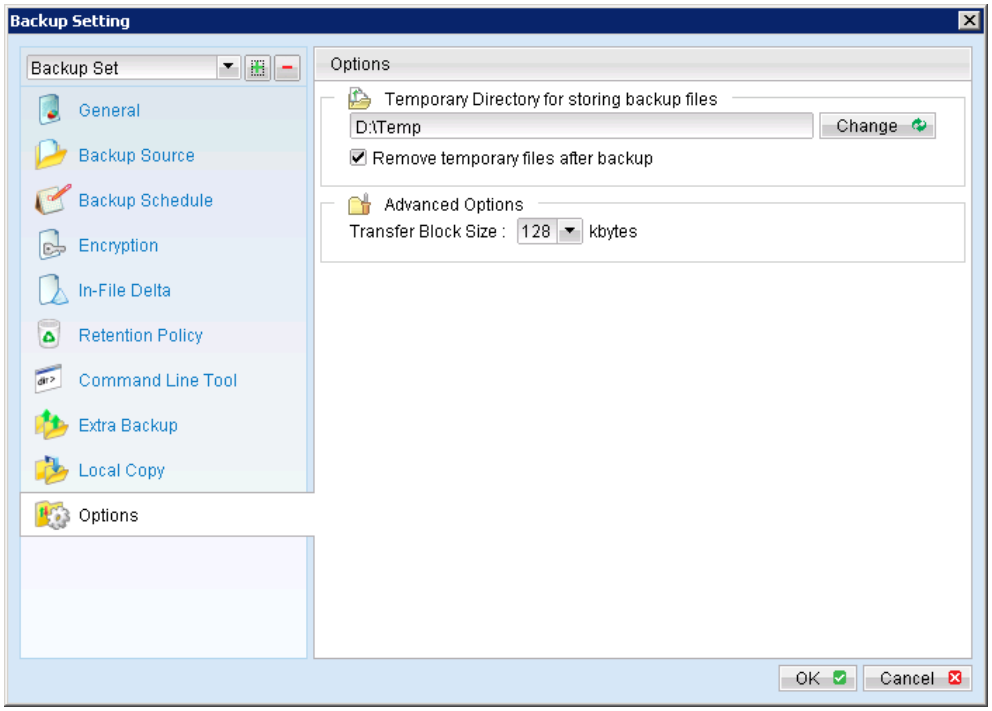
Backup Type	Description
Full	Backup the databases, transaction logs, checkpoint files and then truncates the transaction logs.
Copy	Backup the databases, transaction logs, checkpoint files but does not truncate the transaction logs.
Incremental	Backup the transaction logs to record changes since

	the last full or incremental backup and then truncates the transaction logs.
Differential	Backup the transaction logs to record changes since the last full or incremental backup and does not truncate the transaction logs.

10. Select an encryption setting for your backup set.

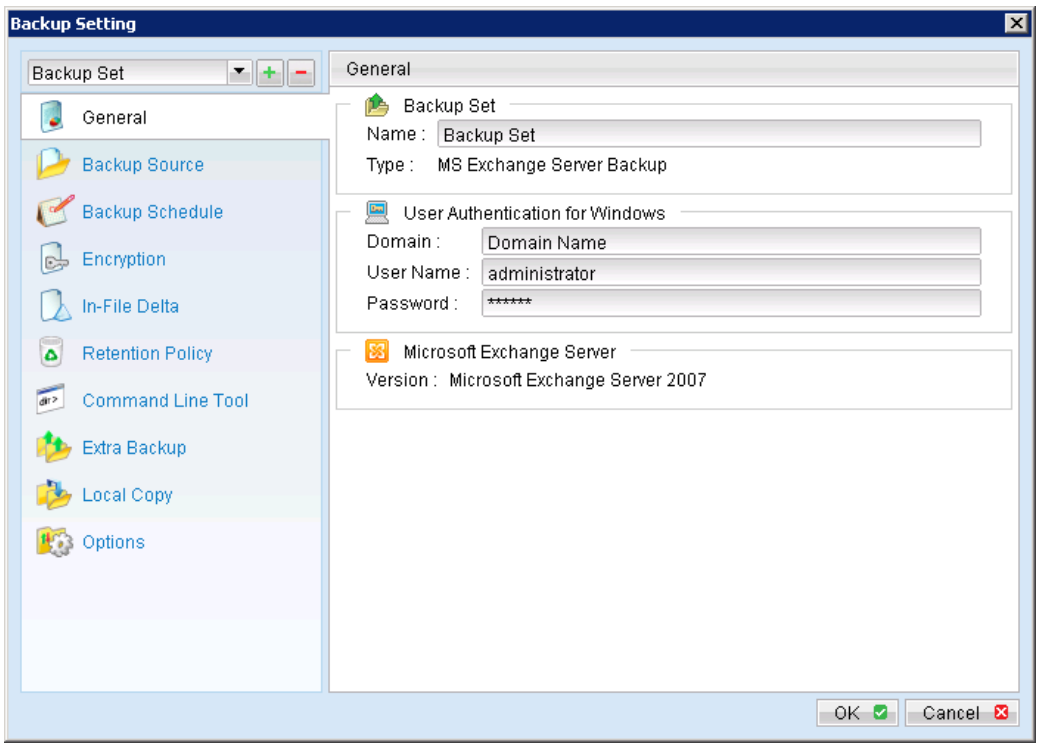
11. Press the [OK] button to complete the configuration of the [New Backup Size Wizard].

12. Configure the temporary backup folder, select [Backup Setting], [Options].

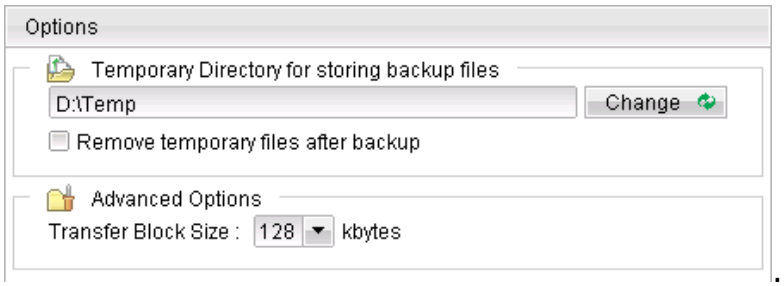


Note:
The temporary directory can be set to a local or network path.

Please be reminded to fill in the [User Authentication for Windows] setting if a network path is selected.

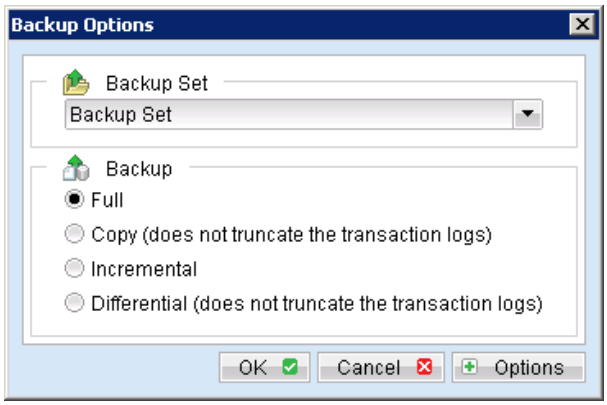


For database specific backup type, data files spooled by the latest backup job can be kept by disabling the [Remove temporary files after backup] option.



13. Scheduled backup will run automatically at the configured schedule time.

14. Click [Backup] button on the left panel to perform a backup immediately.



Menu Items	Description
Backup	Select backup type [Full / Copy / Incremental / Differential].

Further details on Backup Type:

Backup Type	Description
Full	Backup the databases, transaction logs, checkpoint files and then truncates the transaction logs.
Copy	Backup the databases, transaction logs, checkpoint files but does not truncate the transaction logs.
Incremental	Backup the transaction logs to record changes since the last full or incremental backup and then truncates the transaction logs.
Differential	Backup the transaction logs to record changes since the last full or incremental backup and does not truncate the transaction logs.

Important:
For Exchange server with Active Directory installed, a System State backup must be performed regularly with the MS Exchange server backup.

15.5 Restore Microsoft Exchange Server 2010

Refer to the following instructions to restore Microsoft Exchange Server 2010:

1. Prepare the operating system for the Exchange Server restore (if required).

   Install the original version of Windows and Exchange Server (with the same level of service pack installed as in the original system).

2. Restore Windows Active Directory (if required).

   Restore the System State data from OBS, and then restore the System State using WBAdmin.exe.

   Refer to the "How to restore Windows System State" chapter for detailed instruction.

3. Install OBM (if required).

   Refer to the "Installing OBM" chapter for detailed instruction.

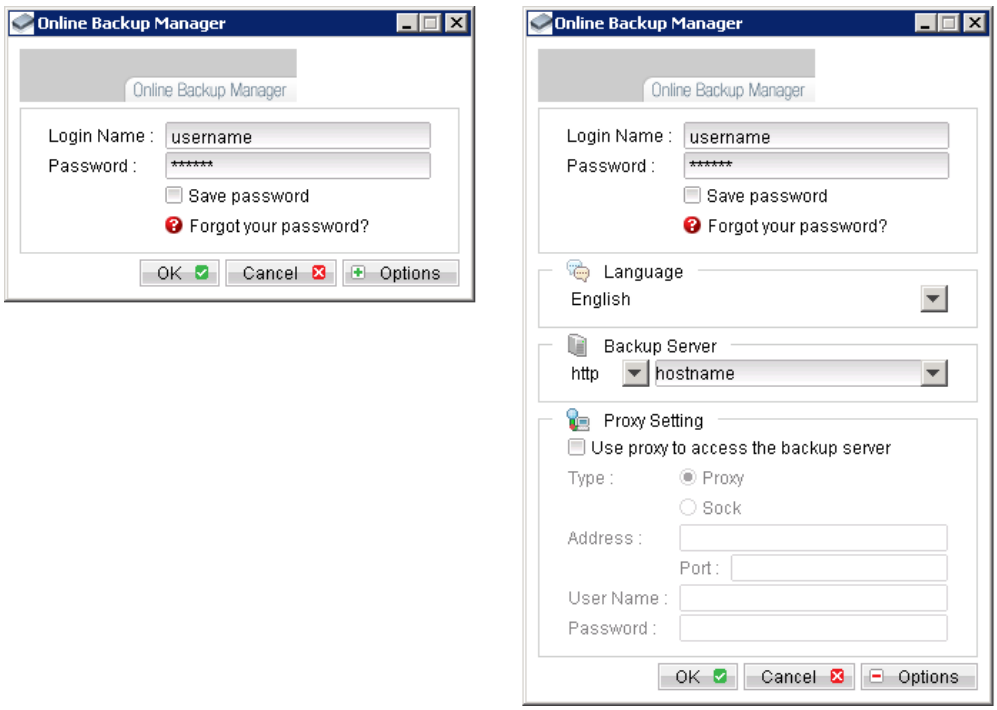
4. Startup the [Microsoft Information Store] services from Windows Services.

5. Continue with the following sections for restore to the original Exchange server, or to a new Exchange server.

Restore Exchange Database to Original Location

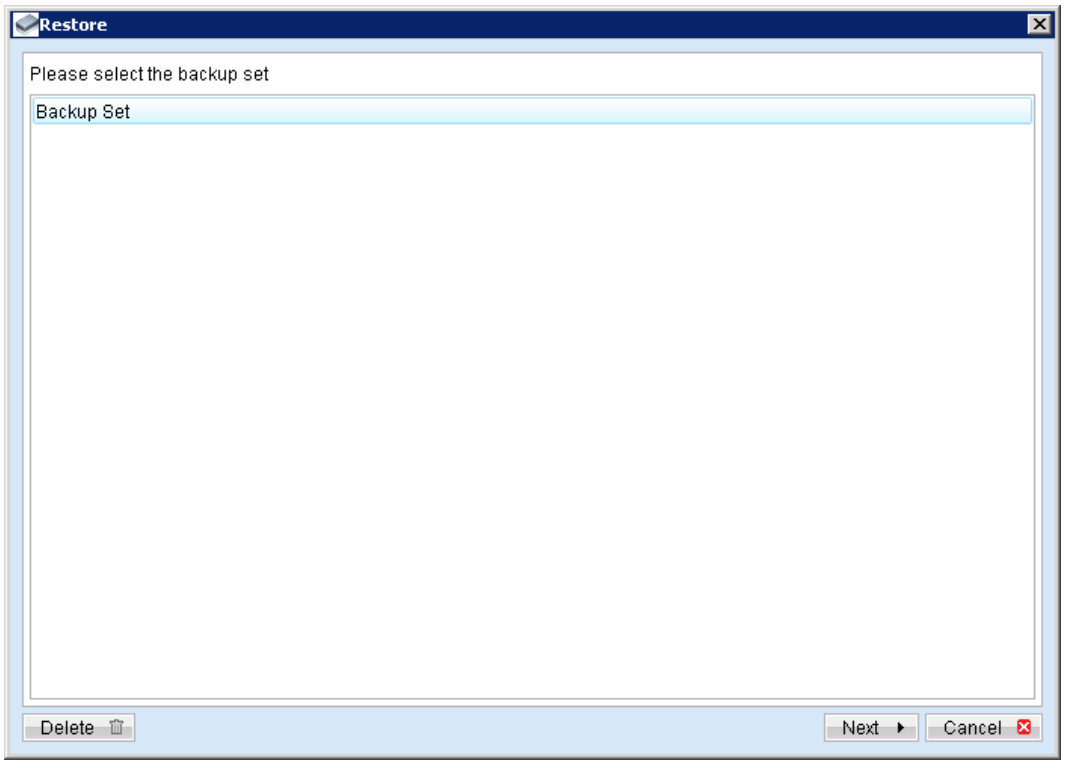
To restore Exchange database to the same Exchange server:

6. Login to the backup application's user interface.

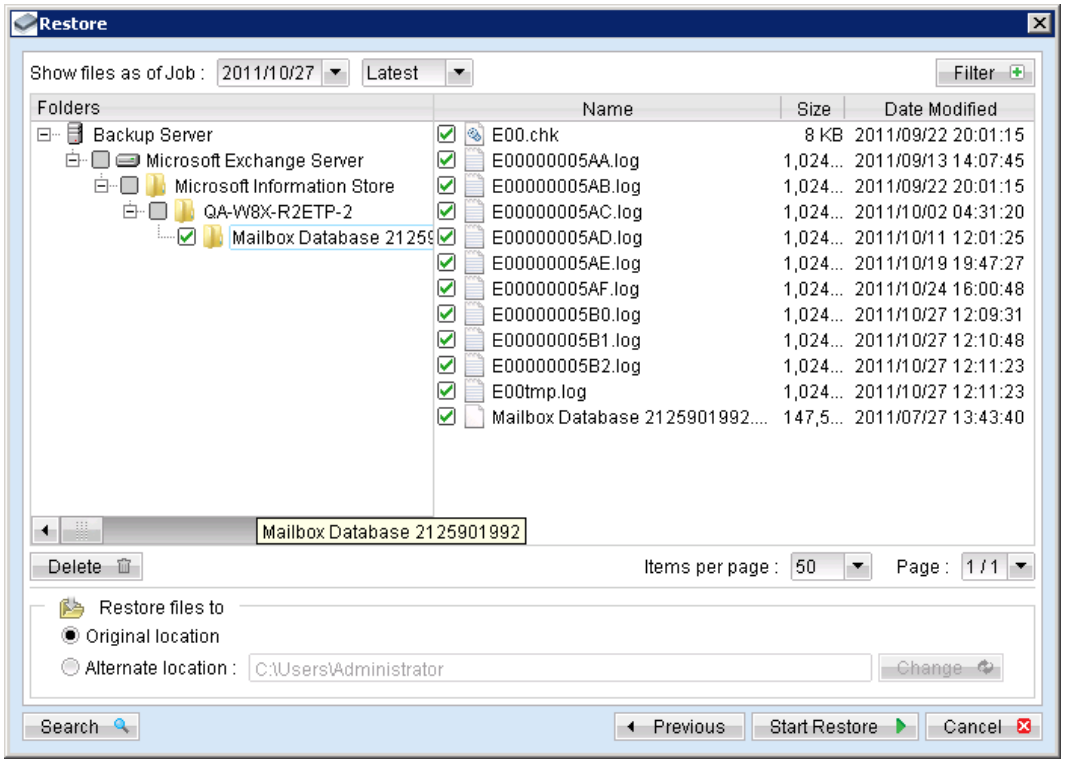


7. Click on the [Restore] button on the left panel.

8. Select the backup set to be restored, and [Next].



9. Expand the server tree, select the database to be restored, and [Original Location] for the [Restore files to] option.



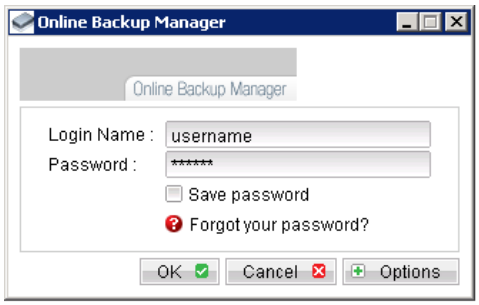
10. Press the [Start Restore] button to begin the restore process.

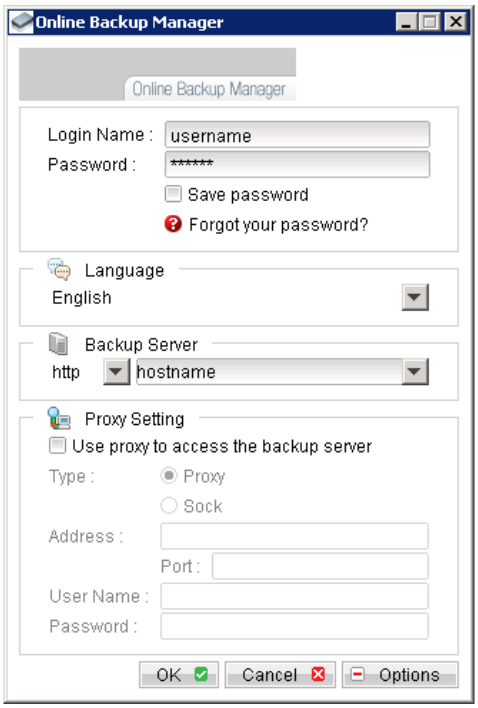
11. The restore process is now completed.

Restore Exchange Database to Alternate Location

To restore Exchange database to a new Exchange server:

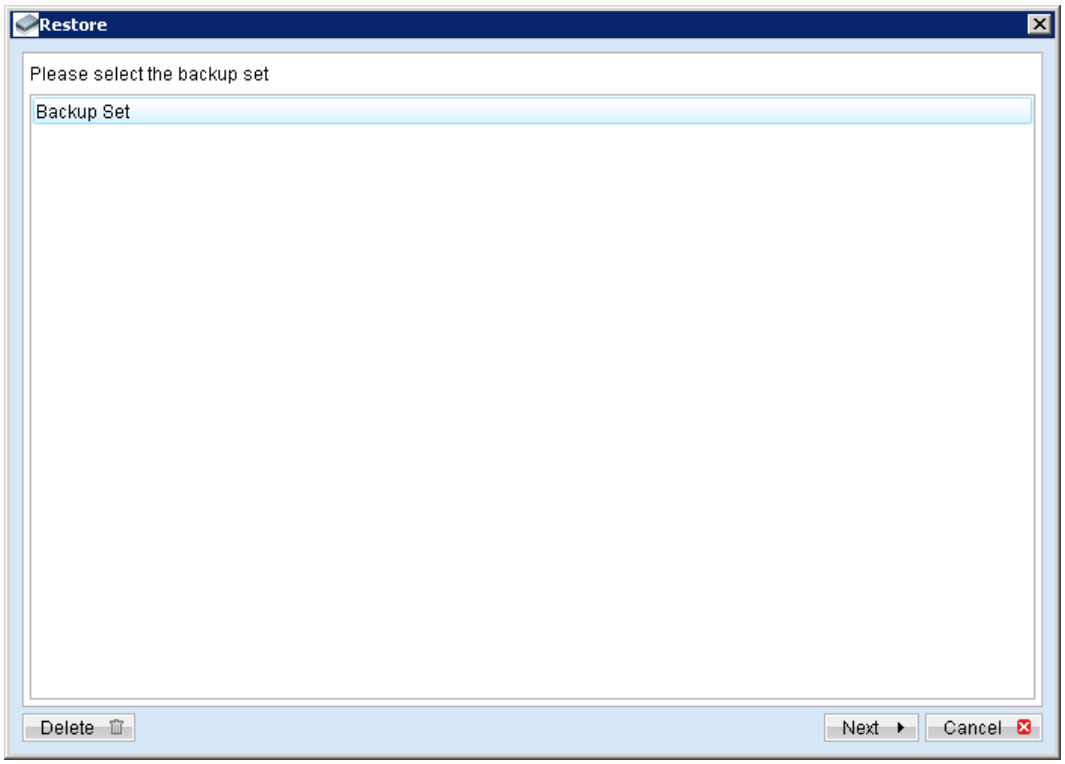
6. Login to the backup application's user interface.



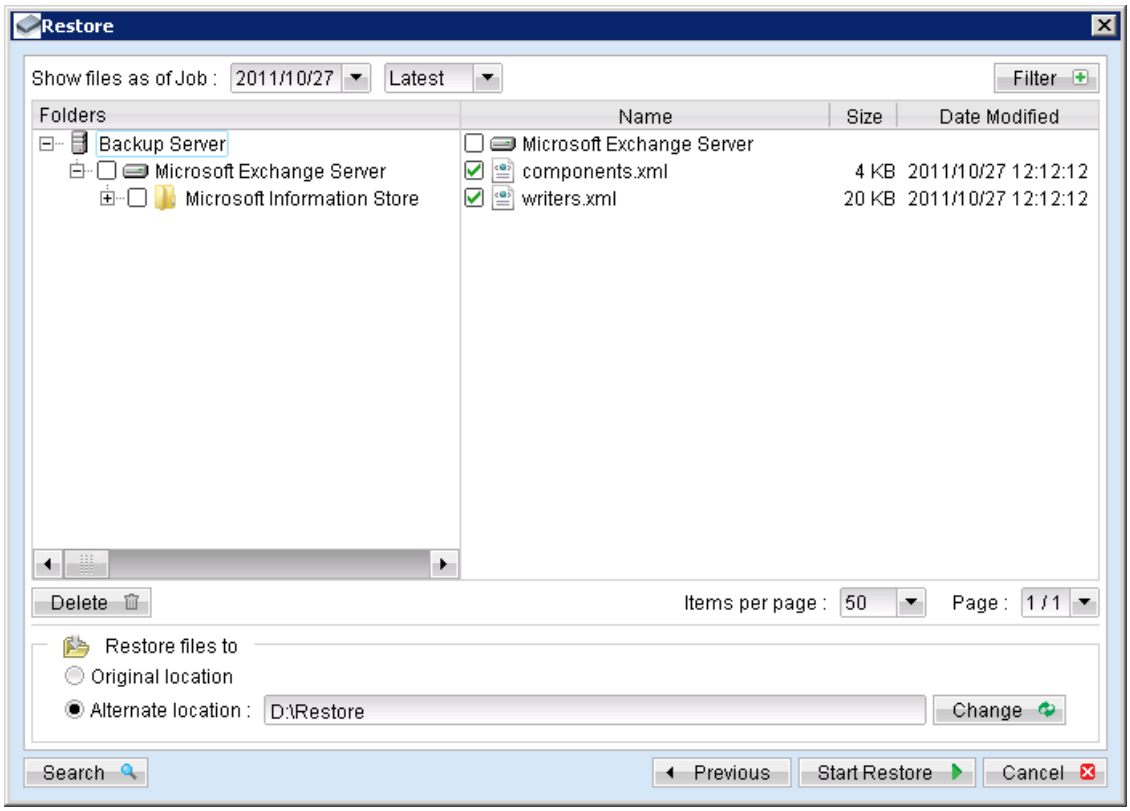


7. Click on the [Restore] button on the left panel.

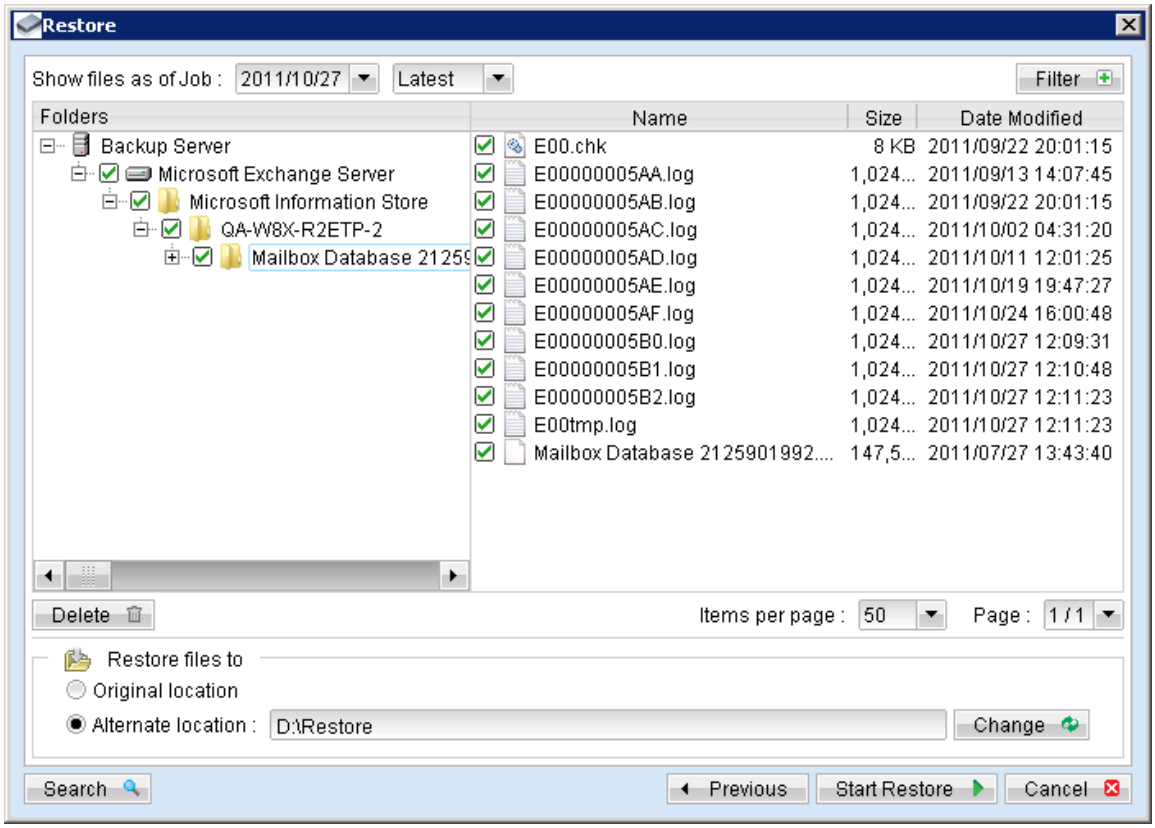
8. Select the backup set to be restored, and [Next].



9. Click on [Backup Server], select [components.xml] and [writers.xml] for restore.



10. Next, select the database to be restored, and select [Alternate location] and browse to the restore destination folder.



11. Please ensure the directory structure is the same as it appears in the File Explorer:

```
-->[Restore Destination]
--------->[Microsoft Exchange Server]
--------->[components.xml]
--------->[writers.xml]
---------------->[Microsoft Information Store]
------------------------------>[Server Name]
---------------------------------------->[Database Name]
```

12. Use the [ExchangeRestore2010.exe] file found from the OBM [bin] directory to restore the database(s).

    ${OBM-Install-Home}\bin\ExchangeRestore2010.exe

13. For restore of all databases from backup data [D:\Restore], the following command can be used.

Exchange server recovery

```
C:\Program Files\OBM\bin>ExchangeRestore2010 D:\Restore
```

14. The restore process is now completed.

16 Brick-Level Backup / Restore Microsoft Exchange Server

This chapter describes in details how to backup and restore individual mail items stored in Microsoft Exchange Server with OBM.

16.1 Supported versions

The MS Exchange Mail Level backup module is supported for the following Exchange versions:

- MS Exchange 2003
- MS Exchange 2007
- MS Exchange 2010 / SP1

For more details, please refer to Help Centre Article:
https://help..com/openArticle.aspx?aid=2323

16.2 Requirements

Please ensure that following requirements are met by the MS Exchange server:

1. OBM is installed on the MS Exchange server.

2. Microsoft Messaging Application Programming Interface (MAPI) is installed on the MS Exchange server.

3. The built in administrator account is must be enabled.

   Important:
   For Windows Small Business Server (SBS) 2003 / 2008 / 2011, the built-in administrator account is disabled by default.

4. The operating system account to be running the Brick-Level backup (e.g. administrator) must have a mailbox and is not hidden from the Global Mailbox List.

5. Backup of Exchange 2010 SP1 in Hosting Mode is currently not supported.

Note:
For OBM version 6.5.4.0 or above, scheduled backup can be performed without changing the scheduler service's log on setting.

Scheduled backup is performed using the operating system account configured in the [User Authentication for Windows] field.

If such setting is not configured, the scheduled backup would precede with the default Local System account (default log on account for OBM scheduler).

In this case, the backup will most likely fail with permission denied error.

16.3 Overview

Brick-Level backup for Microsoft Exchange Server is not designed to fully protect an Exchange Server, but to facilitate easy backup and fast restore of individual emails, contacts or calendars, etc.

A Brick-Level restore cannot fully recover the Information Store after a disaster.

Important:
If used, a Brick-Level Backup must be utilized in conjunction with full Information Store Backup, in order to fully protect the Exchange Server.

16.4 Granting Privileges

Brick-Level backup requires "Full Mailbox Access" permission for the user running OBM.

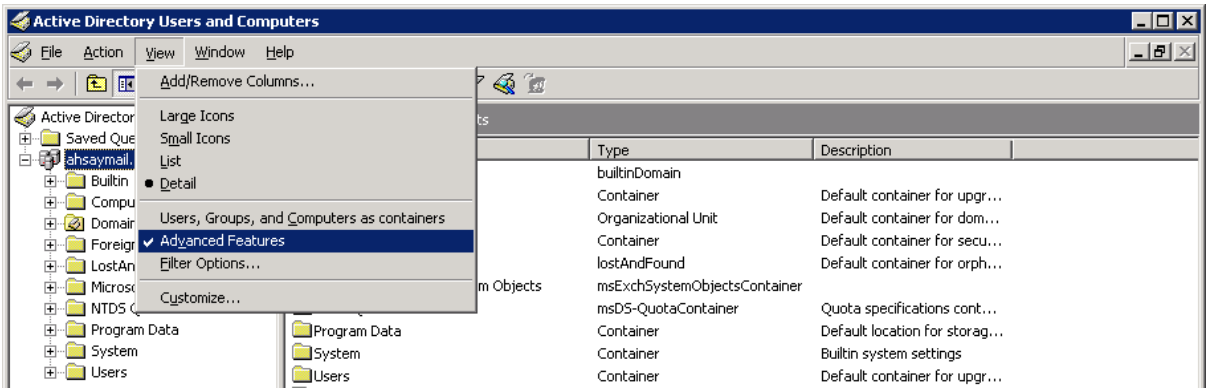
Please refer to the following instruction for granting permission to the operating system account to be running the Brick-Level backup:

For one specific mailbox

Use the following procedure to grant access to Exchange 2003 / 2007 mailbox:

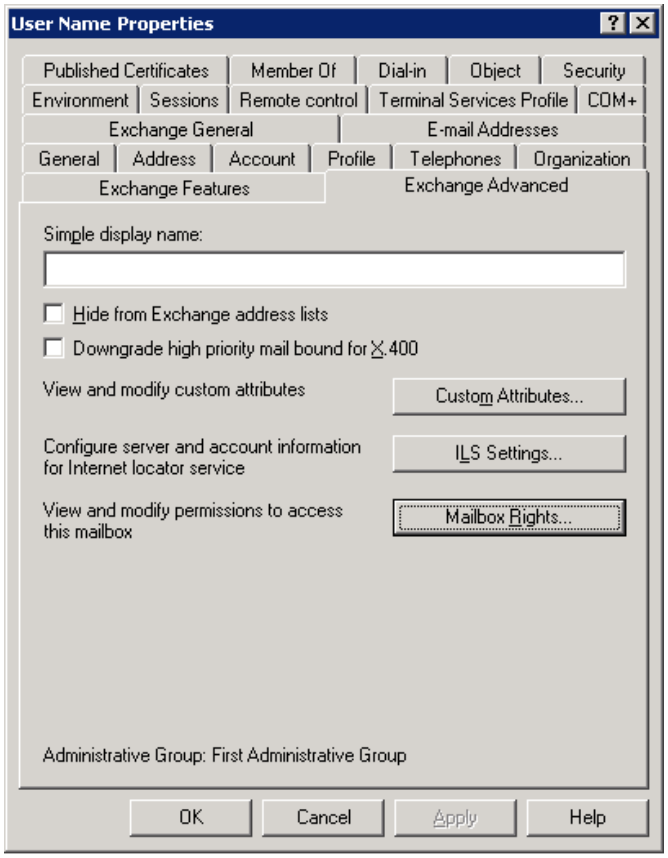
1. Start the [Active Directory Users and Computers] applet.

2. On the [View] menu, ensure that the [Advanced Features] option is selected.

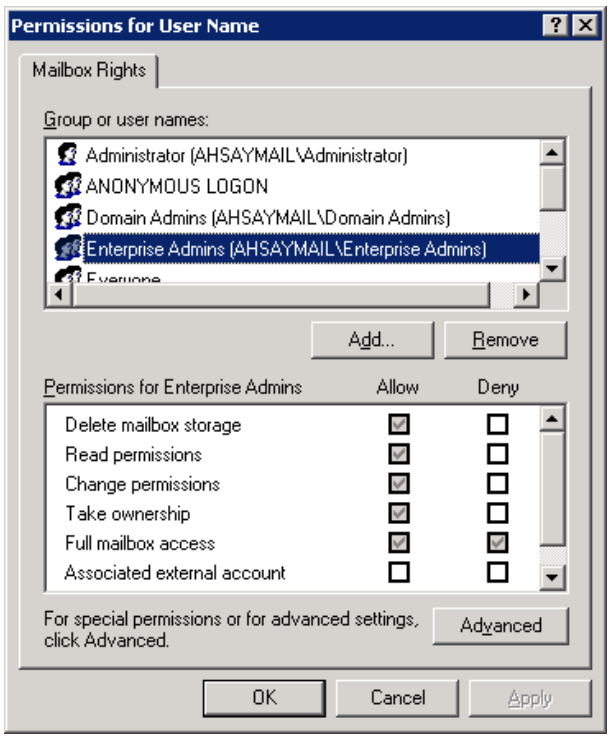


3. Right click the user whose mailbox you want to give permissions to and choose [Properties].

4. On the [Exchange] Advanced tab, click [Mailbox Rights].



5. Notice that the Domain Admins and Enterprise Admins have both been given Deny access to Full Mailbox access.



6. Click [Add], click the user or group who you want to have access to this mailbox, and then click [OK].

7. Ensure that the user or group is selected in the Name box.

8. In the [Permissions] list, click [Allow] next to [Full Mailbox Access], and then click [OK].

9. Click [OK] all the way out.

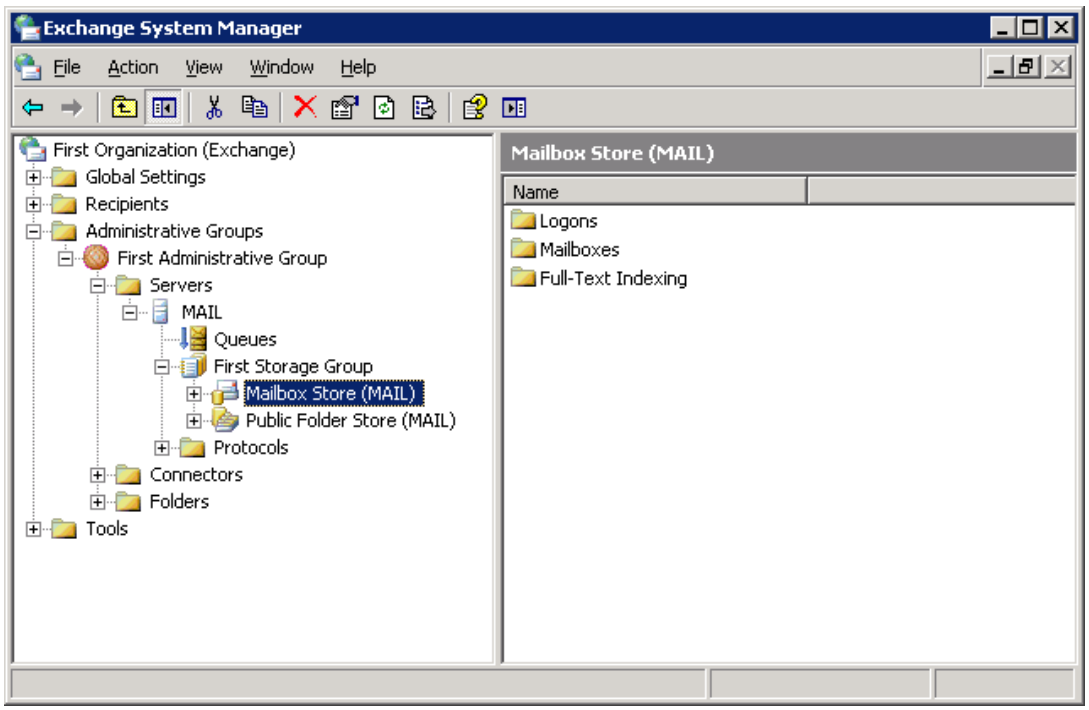
10. Restart the [Microsoft Exchange Information Store] service.

For mailboxes located within a specific mailbox store

Use the following procedure to grant access to Exchange 2003 / 2007 mailbox found on a specific mail store:

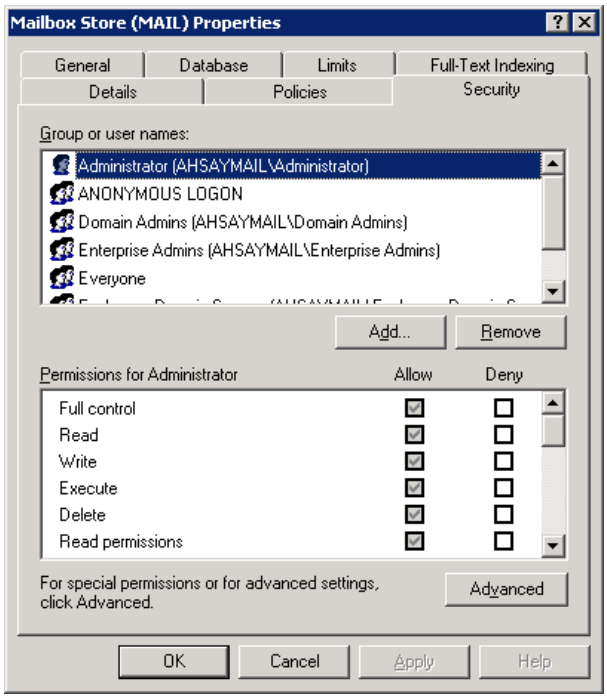
1. Start the [Exchange System Manager] applet.

2. Navigate to the server object within the appropriate Administrative Group.



3. Expand the server object and find the required mailbox store within the appropriate Storage Group. Right click it and choose [Properties].

4. In the [Properties] window, go to the [Security] tab.



5. Click [Add], click the user or group who you want to have access to the mailboxes, and then click [OK].

6. Be sure that the user or group is selected in the Name box.

7. In the [Permission] list, check [Allow] next to [Full Control], and then click [OK].

8. Click [Apply] and [OK].

9. Restart the [Microsoft Exchange Information Store] service.

For mailboxes located within a specific server

For Exchange 2003, please refer to the following instructions:

1. Add an operating system account to the Add an operating system account to the Exchange 2003 server.

   This account must be a member of the following groups in the Active Directory:

   - Domain Users group
   - Administrators group

2. Right click [Exchange System Manager] > [Domain Name] > [Server] > [Exchange Server Name], select [Properties].

3. Choose the [Security] tab.

4. Add the newly created user to the list, and then check the [Full Control] checkbox for this user.

5. Click [OK] all the way out.

6. Reboot the server or restart the [Microsoft Exchange Information Store] service, wait for at least 15 minutes for the changes to be applied to the Exchange server.

For Exchange 2007, please refer to the following instructions:

1. Add an operating system account to the Add an operating system account to the Exchange 2007 server.

   This account must be a member of the following groups:

   - Local Administrators (Built in)
   - Domain Admins group
   - Enterprise Admins group

2. Enter the following command in Exchange Management Shell:

```
Get-MailboxServer | Add-ADPermission -User "%USER%" -
AccessRights GenericAll -ExtendedRights ms-exch-store-
admin,receive-as,send-as -InheritanceType All
```

Example, to grant the permission for local account "system"

```
Get-MailboxServer | Add-ADPermission -User "system" -
AccessRights GenericAll -ExtendedRights ms-exch-store-
admin,receive-as,send-as -InheritanceType All
```

To show added permission for an AD account

```
Get-MailboxServer | Get-ADPermission -User "%USER%"
```

Example, to show added permission for local account "system"

```
Get-MailboxServer | Get-ADPermission -User "system"
```

To remove permission from an AD account

```
Get-MailboxServer | Remove-ADPermission -User "%USER%" -
AccessRights GenericAll -ExtendedRights ms-exch-store-
admin,receive-as,send-as -InheritanceType All
```

Example, to remove permission from local account "system"

```
Get-MailboxServer | Remove-ADPermission -User "minimal" -
AccessRights GenericAll -ExtendedRights ms-exch-store-
admin,receive-as,send-as -InheritanceType All
```

For Exchange Server 2010, please refer to the following instructions:

1. Add an operating system account to the Exchange 2010 server.

   This account must be a member of the following groups:

   - Local Administrators (Built In)
   - Organization Management group (Exchange Security Groups)
   - Domain Admins group
   - Enterprise Admins group

2. Ensure that Update Rollup 3 for Exchange Server 2010 (KB981401) is installed.

3. Enter the following command in Exchange Management Shell:

```
Get-Mailbox | Add-MailboxPermission -User "%USER%" -
AccessRights FullAccess
```

Example:

```
Get-Mailbox | Add-MailboxPermission -User "system" -
AccessRights FullAccess
```

Other useful commands:

Remove permission from an AD account

```
Get-Mailbox | Remove-MailboxPermission -User "%USER%" -
AccessRights FullAccess
```

Example:

```
Get-Mailbox | Remove-MailboxPermission -User "system" -
AccessRights FullAccess
```

To view the mailbox permission of a user

```
Get-Mailbox | Get-MailboxPermission -User "%USER%"
```

Example:

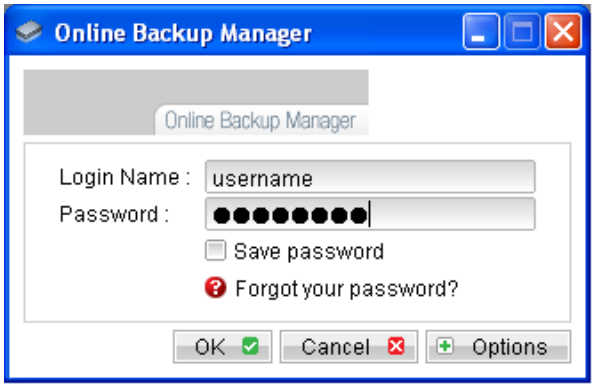
```
Get-Mailbox | Get-MailboxPermission -User "SYSTEM"
```

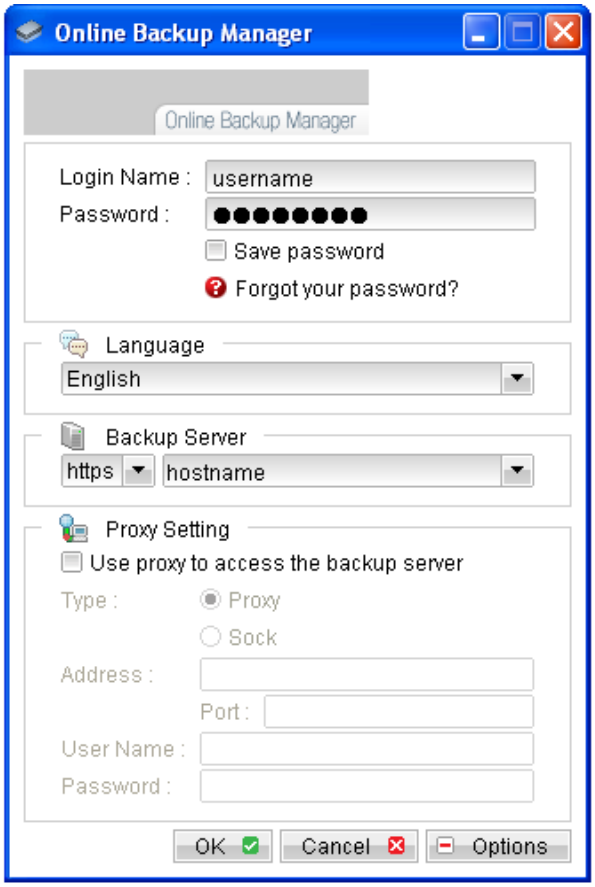
For details on how to troubleshoot for issue encountered when creating a mail level backup set or during backup, please refer to Help Centre Article #2644.

16.5 How to perform Brick-Level backup

Refer to the following instructions to backup individual items within your Microsoft Exchange Server:

1. Login to the backup application's user interface.





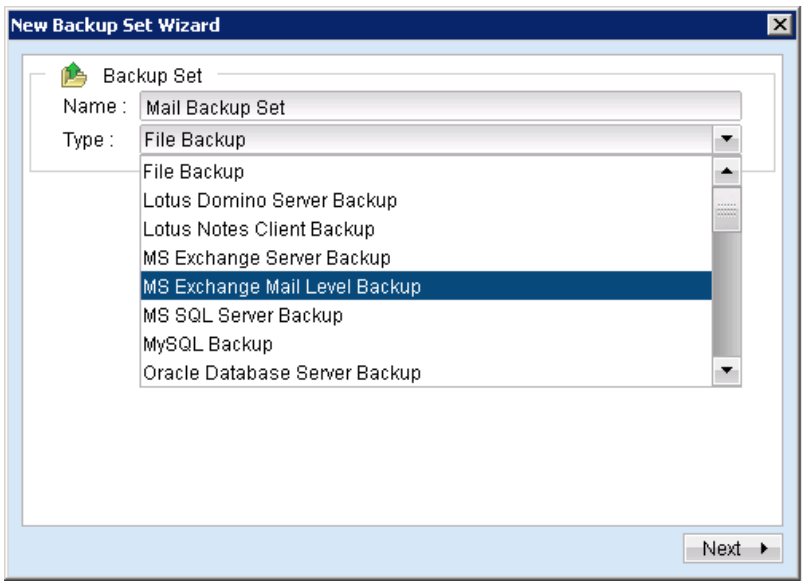
For OBM installation on 64 bit machines, please start the backup application by running the RunOBC32.bat file found under the application installation bin directory:

${OBM-InstallHome}\bin\RunOBC32.bat

2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

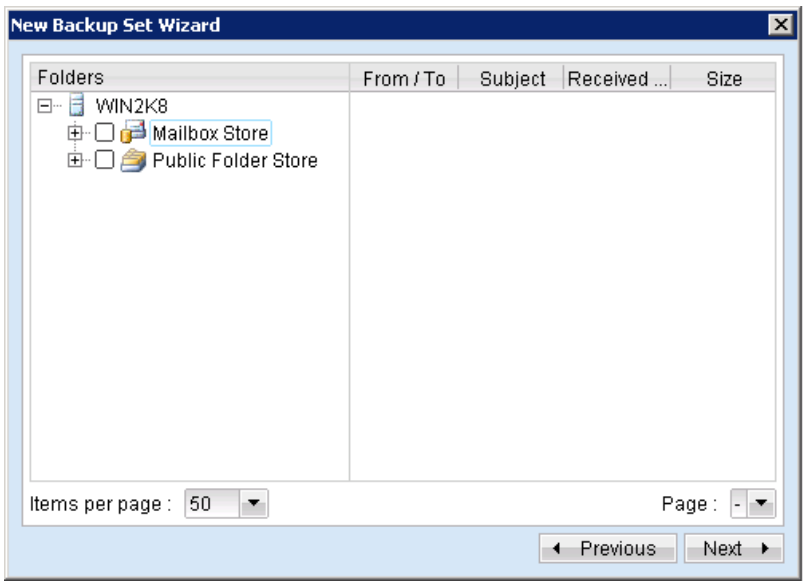
3. Create a MS Exchange mail level backup set by selecting [MS Exchange Mail Level Backup] from the backup set type dropdown menu.

4. Enter the backup set name



5. Select [Next] to proceed.

6. Expand the Mailbox Store to select the corresponding mailboxes for backup.



7. Configure a backup schedule for unattended backups.

   Note:
   Multiple backup schedules of different types can be configured for the same backup set.

8. Select an encryption setting for your backup set.

9. Press the [OK] button to complete the configuration of backup set.

10. Scheduled backup will run automatically at the configured schedule time.

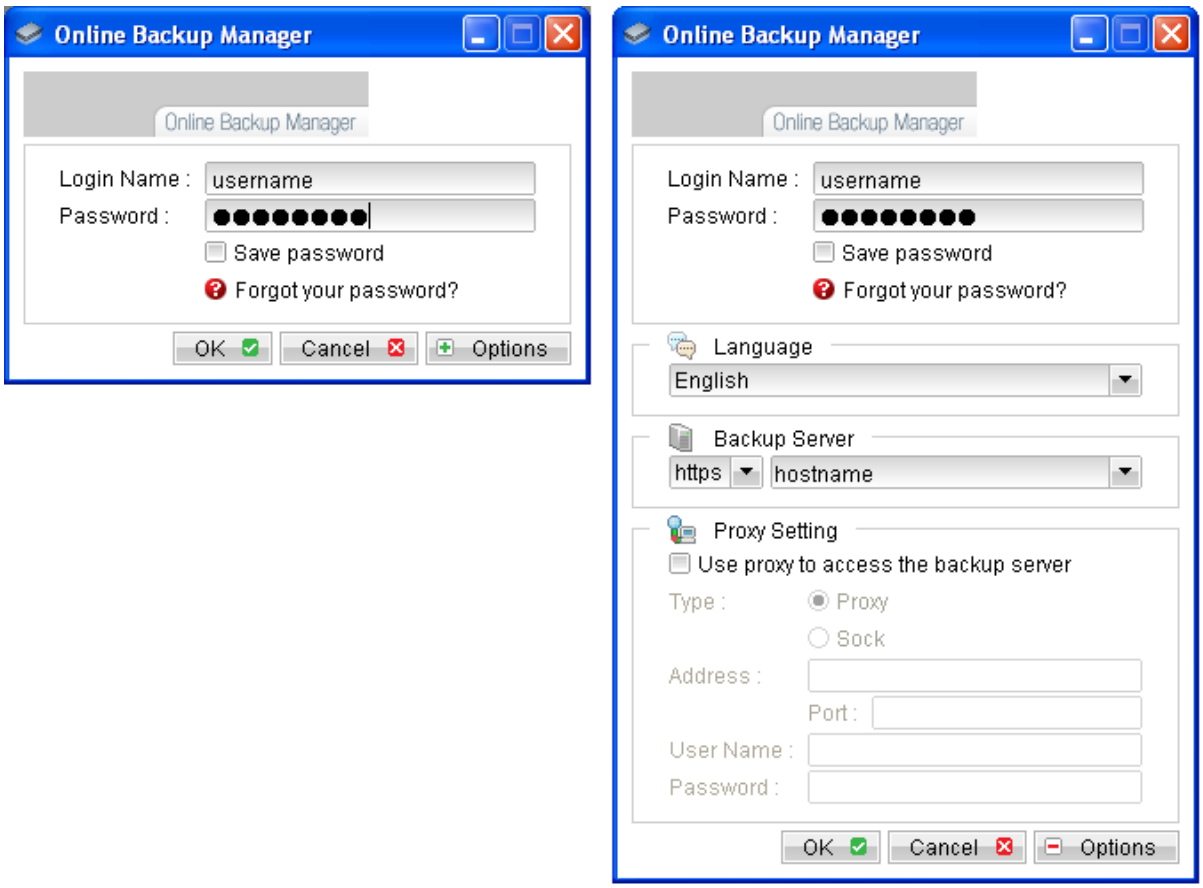
11. Click [Backup] button on the left panel to perform a backup immediately.

16.6 How to perform Brick-Level restore

Refer to the following instructions to restore individual items to the original Microsoft Exchange Server

Note:
Please note that individual Brick-Level backup can only be restored using OBM client (e.g. cannot perform web restore).

1. Login to the backup application's user interface.

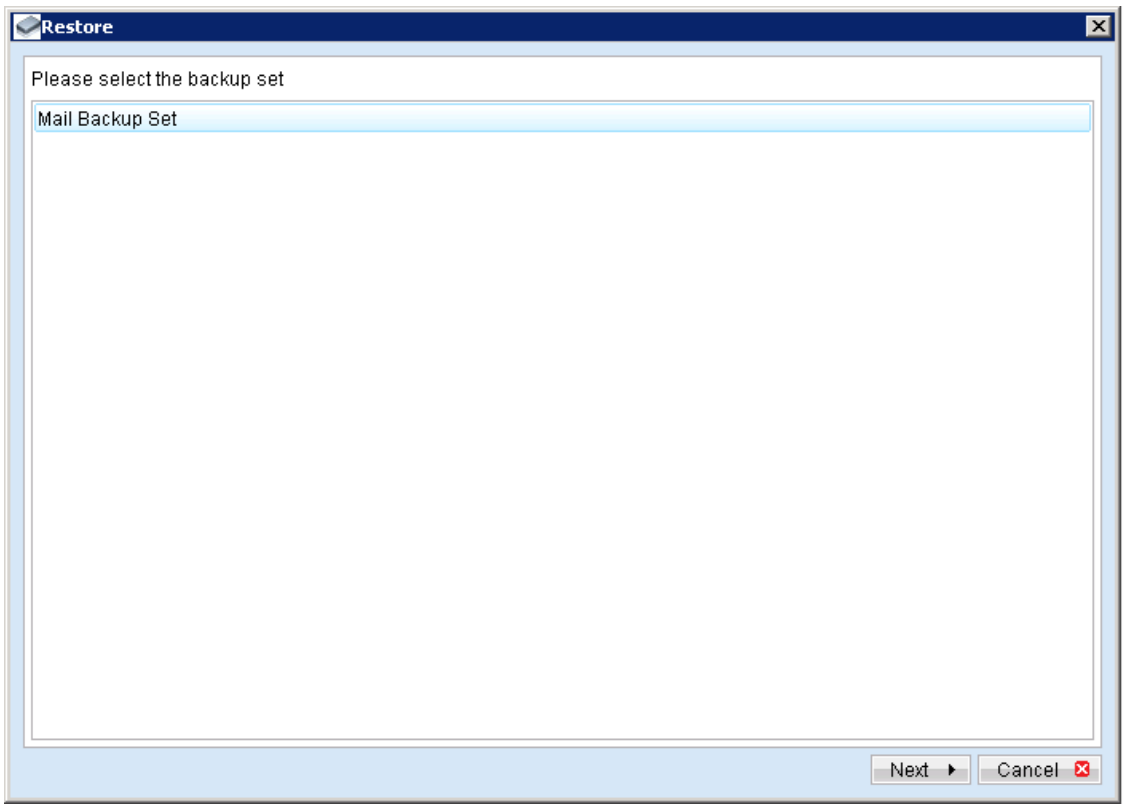


For OBM installation on 64 bit machines, please start the backup application by running the RunOBC32.bat file found under the application installation bin directory:

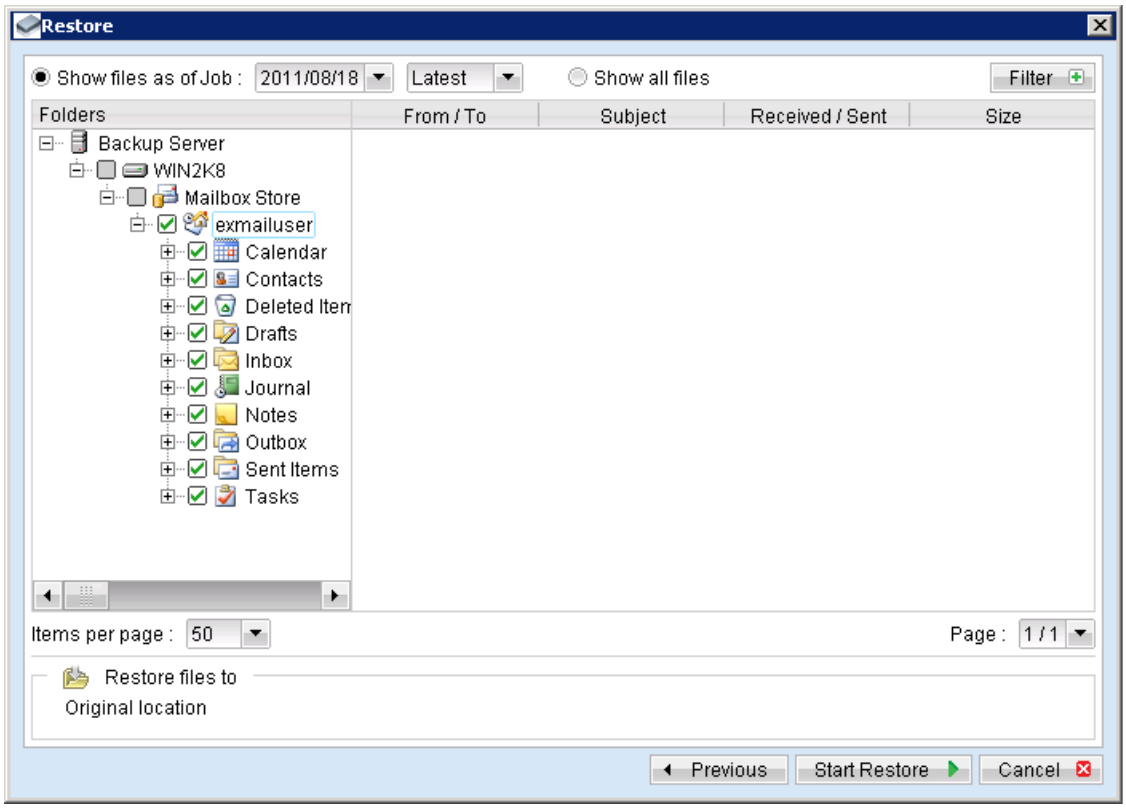
${OBM-InstallHome}\bin\RunOBC32.bat

2. Select the [Restore] button on the OBM main menu.

   Select the corresponding backup set to be restored.



3. Select the individual mail item to be restored.



4. Press the [Start Restore] button to restore.

17 Backup / Restore Oracle Database Server

This chapter describes how to backup and restore Oracle database server.

17.1 Supported versions

The Oracle Database backup module is supported for the following Oracle versions:

- Oracle 10g
- Oracle 11g
- Oracle 11g Release 2

For more details, please refer to Help Centre Article:
https://help..com/openArticle.aspx?aid=2323

17.2 Requirements and recommendations

Please ensure that the following requirements are met by the Oracle database server:

1. OBM is installed on the Oracle database server.

2. The Oracle databases selected for backup will be temporarily spooled to a temp directory before being uploaded to the backup server.

   It is recommended that the temporary directory have disk space of at least 120% of the total database size (e.g. total size of all database files).

3. All database selected for backup, must be in *ARCHIVELOG* mode.

   ARCHIVELOG mode guarantees complete data recoverability, and must be enabled to perform online backups.

   To enable *ARCHIVELOG* mode, please refer to the following instruction:

   - Set the parameters below in the *PFILE* to enable automatic archiving.

```
LOG_ARCHIVE_DEST = ${Storage path of archive redo logs}

LOG_ARCHIVE_FORMAT = 'log%t_%s_%r.arc'

LOG_ARCHIVE_START = true
```

   - Set *ORACLE_SID* to your database *System Identifier (SID)*:

```
Windows:
set ORACLE_SID=${database_SID}

Linux:
export ORACLE_SID=${database_SID}
```

- Connect to database as *SYSDBA*.

```
sqlplus "/ as sysdba"
```

- Shutdown database.

```
SQL> shutdown immediate
```

- Start and mount database.

```
SQL> startup mount
```

- Switch database to archived log mode.

```
SQL> alter database archivelog;
```

- Open database.

```
SQL> alter database open;
```

Example:

```
$ export ORACLE_SID=GDB1

$ sqlplus "/ as sysdba"

SQL*Plus: Release 10.2.0.1.0 - Production on Thu Nov 8
15:08:57 2007

Copyright (c) 1982, 2005, Oracle.  All rights reserved.


Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 -
Production
```

```
With the Partitioning, OLAP and Data Mining options

SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.

SQL> startup mount
ORACLE instance started.

Total System Global Area  285212672 bytes
Fixed Size                  1218992 bytes
Variable Size              96470608 bytes
Database Buffers          184549376 bytes
Redo Buffers                2973696 bytes
Database mounted.

SQL> alter database archivelog;

Database altered.

SQL> alter database open;

Database altered.
```

4. Grant *JAVASYSPRIV* to the system account.

```
SQL> grant javasyspriv to system;
```

Example:

```
SQL> grant javasyspriv to system;
Grant succeeded.
```

5. Archived logs are not deleted automatically after an Oracle database backup by OBM.

   When necessary, database administrator may consider deleting the backed up archived log manually.

17.3 Overview

The following steps are performed during a backup job:

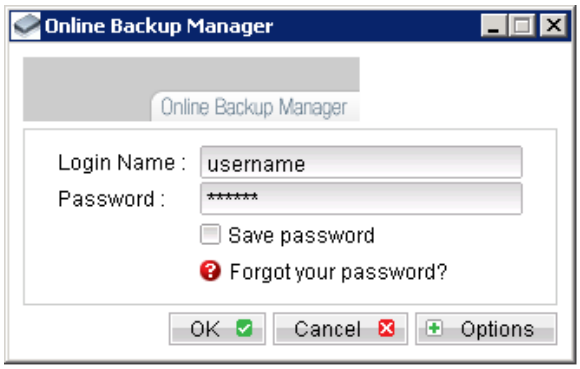
1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Connection to the Oracle database is established using *SQL*NET*.
4. For backup type [Database Backup], commands are issued for the following data to be spooled to the temporary spool path:
   - All tablespace selected for backup
   - All non default initialization parameters
   - All control files
   - All archived log files
5. For backup type [Archived Log Backup], commands are issued for archived logs to be spooled to the temporary spool path.
6. Server and local file lists are compared to determine which file will be uploaded.
7. Delta file is generated for modified file (if necessary).
8. Data are encrypted, compressed, and uploaded to the backup server.
9. Data are removed from the temporary spool path.
10. Backup completed successfully.

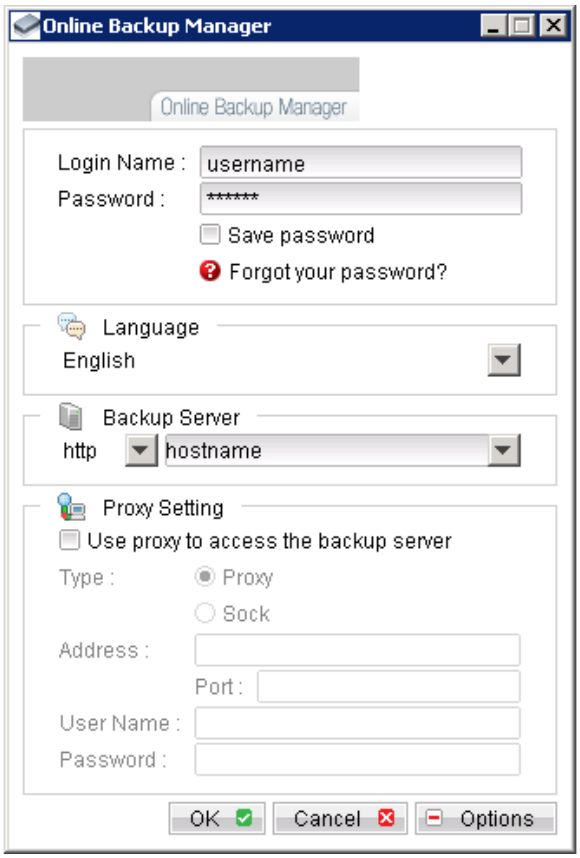
17.4 How to backup an Oracle database (Windows)

Refer to the following instructions to backup Oracle database installation on Windows:

1. Login to the backup application's user interface.

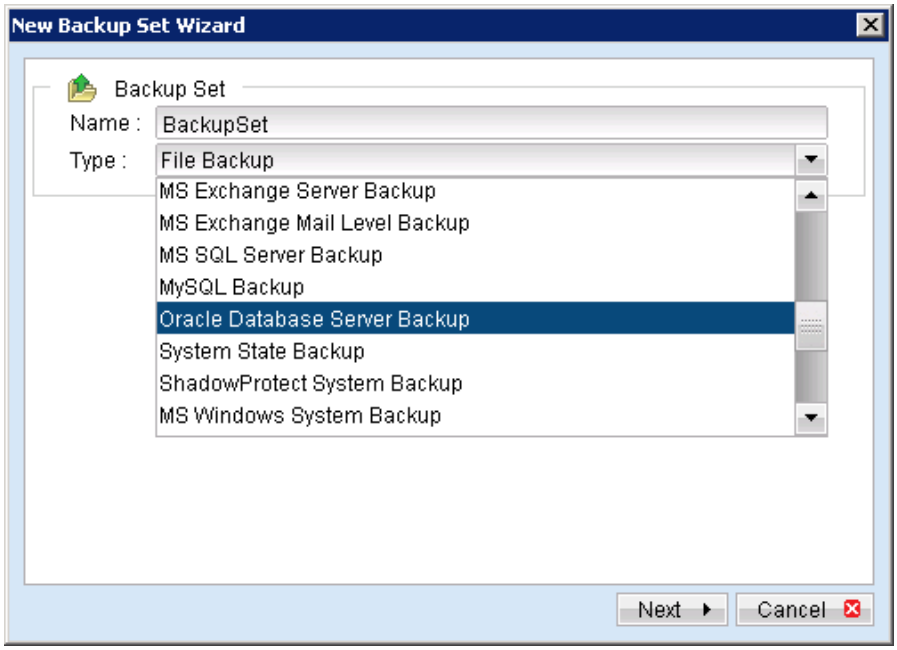
   Double-click on the OBM desktop icon or right-click on the system tray icon:





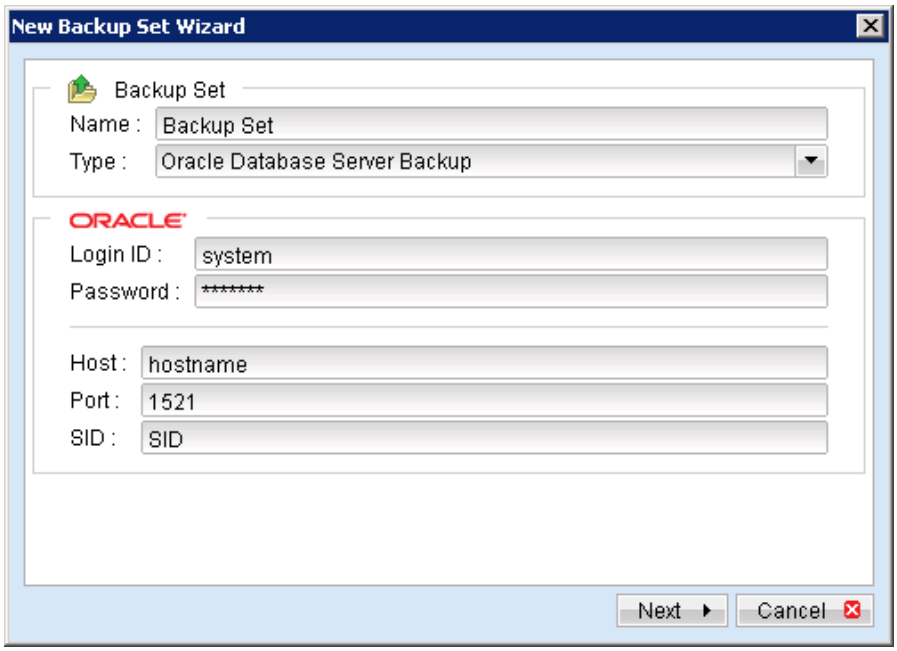
   Note:
   OBM must be installed on the Oracle database server.

2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.



3. Create an Oracle Database Server Backup set by selecting [Oracle Database Server Backup] from the backup set type dropdown menu.

4. Enter the corresponding information required:

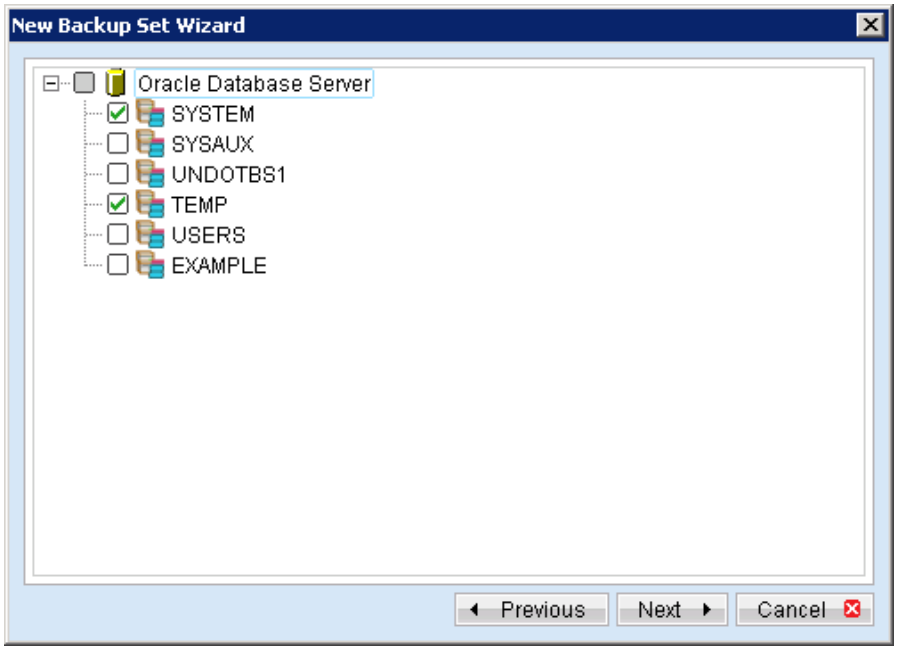


Menu Items	Description
Name	Enter a backup set name of your choice.
Type	Select backup set type [Oracle Database Server Backup].
Login ID	Enter the Login ID of the Oracle system account.

Password	Enter the password of the Oracle system account.
Host	Enter the IP address or hostname of the Oracle database server. Note: OBM must be installed on the Oracle database server.
Port	Enter the Oracle TNS port.
SID	Enter the Oracle SID.

5. Select [Next] to proceed.

6. Select the corresponding tablespace for backup.



7. Configure a backup schedule for unattended backups.

   Note:
   Multiple backup schedules of different types can be configured for the same backup set.

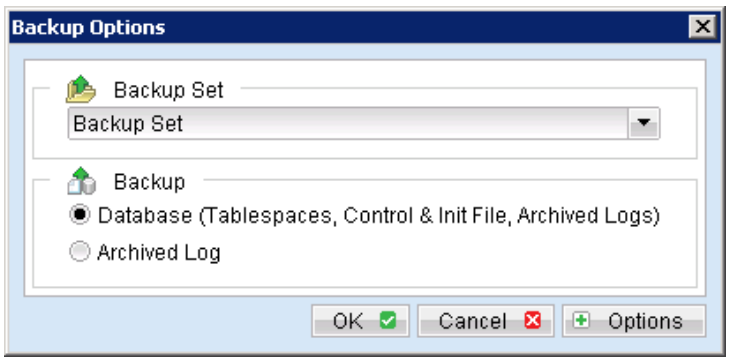
8. Select an encryption setting for your backup set.

9. Press the [OK] button to complete the configuration of backup set.

10. Scheduled backup will run automatically at the configured schedule time.

11. Click [Backup] button on the left panel to perform a backup immediately.

12. Select the backup type to be performed:



Menu Items	Description
Database (Tablespaces, Control & Init File, Archived Logs)	Backup the following: All tablespace selected for backup All non-default initialization parameters All control files All archived log files
Archived Log	Backup the archived log.

17.5 How to backup an Oracle database (Linux)

Refer to the following instructions to backup Oracle database installation on Linux:

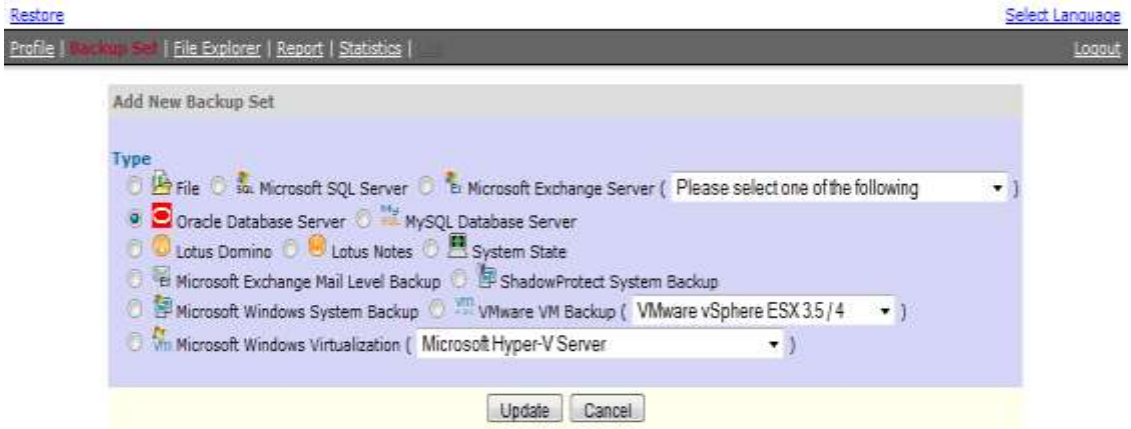
1. Install OBM on the Oracle database server.

   Note:
   OBM must be installed on the Oracle database server.

2. Create a new Oracle Database Server Backup set on the web interface.

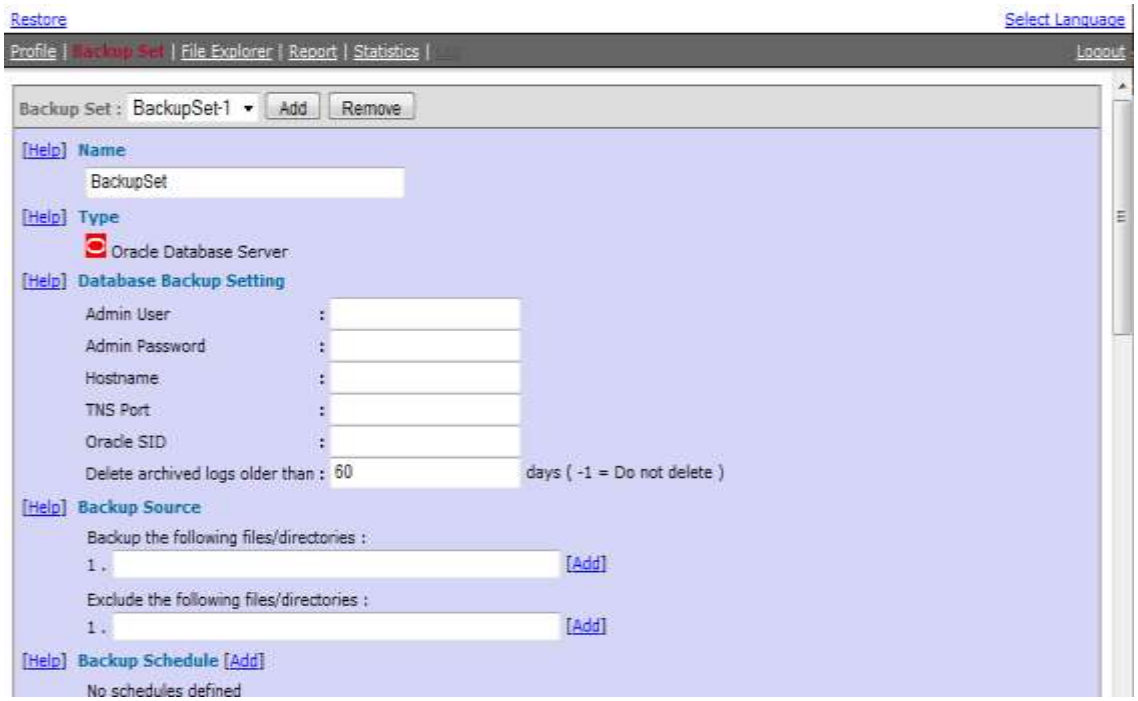
3. Login to the OBS web console, select [Backup Set].

4. Press the [Add] button to access the Add New Backup Set menu.



5. Select the [Oracle Database Server] radio button and [Update].

6. Enter the Name and Database Backup Setting required:

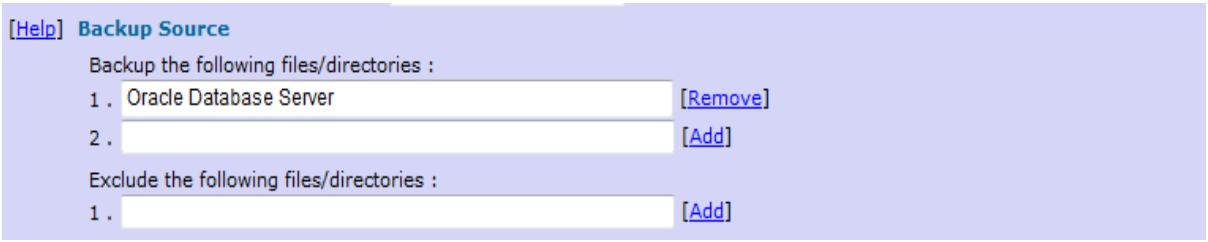


Menu Items	Description
Name	Enter a backup set name of your choice.
Admin User	Enter the Login ID of the Oracle system account.
Admin Password	Enter the password of the Oracle system account.
Hostname	Enter the IP address or hostname of the Oracle database server. Note: OBM must be installed on the Oracle database server.

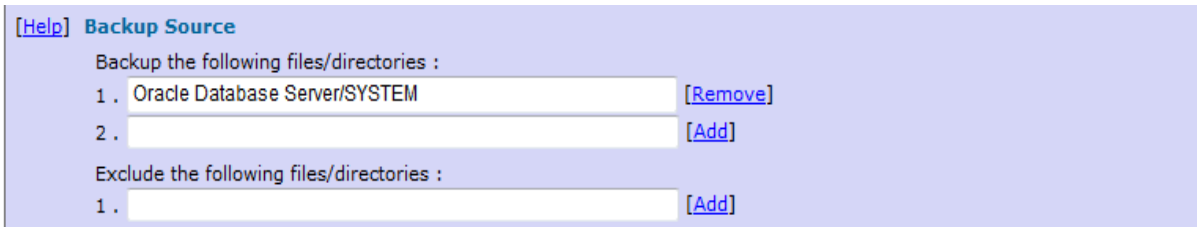
TNS Port	Enter the Oracle TNS port.
Oracle SID	Enter the Oracle SID.
Delete archived logs older than	Option to delete archived log exceeded x days.

7. Enter the Backup Source required:

   To backup all tablespaces, enter 'Oracle Database Server' in the [Backup the following files/directories] field:



   To backup or exclude individual tablespace, enter 'Oracle Database Server/Database_Name' (e.g. Oracle Database Server/SYSTEM):



8. Configure a backup schedule for unattended backups.

   Note:
   Multiple backup schedules of different types can be configured for the same backup set.

9. Press the [Update] button to save the newly created backup set.

10. Login to the Oracle database server with OBM installed.

11. Start the Configurator.sh script by accessing the backup client installation bin folder:

```
>sh OBM_HOME/bin/Configurator.sh
```

12. Follow the instructions provided in the Configurator to complete the configuration of the backup set.

For Linux with GUI installed, backup set can also be created using the OBM user interface, similar to the procedures provided in the Windows section.

Launch the OBM user interface:

```
>sh OBM_HOME/bin/RunOBC.sh
```

13. Scheduled backup will run automatically at the configured schedule time.

14. To perform a backup immediately, execute the RunBackupSet.sh script with the backup set name or ID:

```
>sh OBM_HOME/bin/RunBackupSet.sh BackupSet_Name
```

Important:
Before executing the script, please edit the BACKUP_TYPE parameter within the RunBackupSet.sh script file from -

*BACKUP_TYPE="**FILE**"*

to

*BACKUP_TYPE="**DATABASE**"*

17.6 How to restore an Oracle database

Refer to the following instructions to restore Oracle database:

1. Install OBM on the Oracle database server (if required).
2. Restore the Oracle database backup files from the OBS server.
3. For restore of an existing database, first shutdown the database:
   - Set *ORACLE_SID* to your database *System Identifier (SID)*:

```
Windows:
set ORACLE_SID=${database_SID}

Linux:
export ORACLE_SID=${database_SID}
```

   - Connect to database as *SYSDBA*.

```
sqlplus "/ as sysdba"
```

   - Shutdown the database.

```
SQL> shutdown immediate
```

Example:

```
$ export ORACLE_SID=GDB1

$ sqlplus "/ as sysdba"

SQL*Plus: Release 10.2.0.1.0 - Production on Thu Nov 8
17:04:57 2007

Copyright © 1982, 2005, Oracle. All right reserved.

Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 -
Production With the Partitioning, OLAP and Data Mining
options

SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.
```

4. For restore of a non-existing database, first create a password file:

```
orapwd file=$ORACLE_HOME/dbs/orapw${database_SID}
password=${password}
```

Example:

$ orapwd file=/oracle/OraHome1/dbs/orapwBGDB1 password=pwd123

5. Place the restored backup files to their original directory path:

   Control files, datafiles and archived logs are stored on OBS along with their full path information.

   For example with the data restored to the directory /obm_restore:

```
/obm_restore/Oracle Database
Server/oracle/product/10.2.0/db_1/admin/GDB1/

/obm_restore/Oracle Database
Server/oracle/product/10.2.0/db_1/dbs/initGDB1.ora

/obm_restore/Oracle Database
Server/oracle/product/10.2.0/db_1/dbs/spfileGDB1.ora

/obm_restore/Oracle Database
Server/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1

/obm_restore/Oracle Database
Server/oracle/product/10.2.0/db_1/oradata/GDB1
```

   These files should be moved to:

```
/oracle/product/10.2.0/db_1/admin/GDB1/

/oracle/product/10.2.0/db_1/dbs/initGDB1.ora

/oracle/product/10.2.0/db_1/dbs/spfileGDB1.ora

/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/

/oracle/product/102.0/db_1/oradata/GDB1/
```

6. Rename database files (for database restore to a new location):

   - Modify the *PFILE* file to update file path.

     Modify all file paths to reflect the change to the new location, and then save.

     For example from:

```
background_dump_dest = /oracle/OraHome1/admin/GDB2/bdump

control_files =
(/oracle/OraHome1/oradata/GDB2/control01.ctl,
/oracle/OraHome1/oradata/GDB2/control02.ctl,
/oracle/OraHome1/oradata/GDB2/control03.ctl)

core_dump_dest = /oracle/OraHome1/admin/GDB2/cdump

user_dump_dest = /oracle/OraHome1/admin/GDB2/udump
```

     Change to:

```
background_dump_dest =
/new_db_location/OraHome1/admin/GDB2/bdump

control_files =
(/new_db_location/OraHome1/oradata/GDB2/control01.ctl,
/new_db_location/OraHome1/oradata/GDB2/control02.ctl,
/new_db_location/OraHome1/oradata/GDB2/control03.ctl)

core_dump_dest =
/new_db_location/OraHome1/admin/GDB2/cdump

user_dump_dest =
/new_db_location/OraHome1/admin/GDB2/udump
```

   - Quote the values of *Dispatchers* as a single argument:

```
Dispatchers = "(PROTOCOL=TCP) (SERVICE=GDB1XDB)"
```

   - Delete the *SPFILE* file.

   - Set *ORACLE_SID* to your database *System Identifier (SID)*.

```
Windows:
set ORACLE_SID=${database_SID}
```

```
Linux:
export ORACLE_SID=${database_SID}
```

- Run *SQL Plus* and connect to the database as *SYSDBA*

```
sqlplus "/ as sysdba"
```

- Start and mount the database.

```
SQL> startup mount
```

- Create a backup of the control file to trace file.

```
SQL> alter database backup controlfile to trace as
'New_DB_Location/CONTROL.TRC' reuse;
```

- Rename each of datafile, log file and temp file.
- Open the newly created trace file and check for the filename of each datafile, log file and tempfile.

  Rename each of these files:

```
SQL> alter database rename file 'xxx' to 'yyy';

Where xxx is the old filename found in the trace file, and
yyy is the new filename with the updated path.
```

  Example:

```
SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/system01.dbf' to
'/new_db_location/oradata/GDB1/system01.dbf';

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/undotbs01.dbf'
to '/new_db_location/oradata/GDB1/undotbs01.dbf';

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/sysaux01.dbf' to
'/new_db_location/oradata/GDB1/sysaux01.dbf';
```

```
SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/users01.dbf' to
'/new_db_location/oradata/GDB1/users01.dbf';

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/TS1' to
'/new_db_location/oradata/GDB1/TS1';

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/redo01.log' to
'/new_db_location/oradata/GDB1/redo01.log';

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/redo02.log' to
'/new_db_location/oradata/GDB1/redo02.log';

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/redo03.log' to
'/new_db_location/oradata/GDB1/redo03.log';

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/temp01.dbf' to
'/new_db_location/oradata/GDB1/temp01.dbf';
```

Example:

```
$ export ORACLE_SID=GDB1

$ sqlplus "/ as sysdba"

SQL*PLUS: Release 10.2.0.1.0 - Production on Fri Nov 9
17:50:30 2007

Copyright © 1982, 2005, Oracle. All rights reserved.

Connected to an idle instance.

SQL> startup mount

ORACLE instance started.

Total System Global Area 285212672 bytes
Fixed Size 1218992 bytes
Variable Size 92276304 bytes
Database Buffers 188743680 bytes
Redo Buffers 2973696 bytes
Database mounted.

SQL> alter database backup controlfile to trace as
'/new_db_location/control.trc' reuse;

Database altered.

SQL> alter database rename file
```

```
'/oracle/product/10.2.0/db_1/oradata/GDB1/system01.dbf' to
'/new_db_location/oradata/GDB1/system01.dbf';

Database altered.

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/undotbs01.dbf' to
'/new_db_location/oradata/GDB1/undotbs01.dbf';

Database altered.

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/sysaux01.dbf' to
'/new_db_location/oradata/GDB1/sysaux01.dbf';

Database altered.

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/users01.dbf' to
'/new_db_location/oradata/GDB1/users01.dbf';

Database altered.

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/TS1' to
'/new_db_location/oradata/GDB1/TS1';

Database altered.

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/redo01.log' to
'/new_db_location/oradata/GDB1/redo01.log';

Database altered.

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/redo02.log' to
'/new_db_location/oradata/GDB1/redo02.log';

Database altered.

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/redo03.log' to
'/new_db_location/oradata/GDB1/redo03.log';

Database altered.

SQL> alter database rename file
'/oracle/product/10.2.0/db_1/oradata/GDB1/temp01.dbf' to
'/new_db_location/oradata/GDB1/temp01.dbf';

Database altered.
```

7. Restore the database.

   Perform the following steps to restore database using Recovery Manager:

   - Set *ORACLE_SID* to your database *System Identifier (SID)*.

```
Windows:
set ORACLE_SID=${database_SID}

Linux:
export ORACLE_SID=${database_SID}
```

   - Run *Oracle Recovery Manager (rman)* and connect to the target database.

```
rman target /
```

   - Start and mount the database.

```
RMAN> startup mount
```

   - Apply all transactions from the archived log files to the last sequence.

```
RMAN> recover database until sequence=4 thread=1;
```

     The above command assumes that the sequence number of the last archived log is 3.

     The sequence numbers can be found on the filename of the archived log:

```
${Oracle_Home}/dbs/ol_mf_1_2_3xxxxxxx_.arc
${Oracle_Home}/dbs/ol_mf_1_3_3xxxxxxx_.arc
```

   - Open the database.

```
RMAN> alter database open resetlogs;
```

Example:
$ export ORACLE_SID=GDB1

```
$ rman target /

Recovery Manager: Release 10.2.0.1.0 - Production on Thu Nov
8 17:46:27 2007

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

connected to target database (not started)

RMAN> startup mount

Oracle instance started
database mounted

Total System Global Area     285212672 bytes

Fixed Size                     1218992 bytes
Variable Size                113247824 bytes
Database Buffers             167772160 bytes
Redo Buffers                   2973696 bytes

RMAN> recover database until sequence=4 thread=1;

Starting recover at 08-NOV-07
Starting implicit crosscheck backup at 08-NOV-07
using target database control file instead of recovery
catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=157 devtype=DISK
Finished implicit crosscheck backup at 08-NOV-07

Starting implicit crosscheck copy at 08-NOV-07
using channel ORA_DISK_1
Finished implicit crosscheck copy at 08-NOV-07

searching for all files in the recovery area
cataloging files...
cataloging done

List of Cataloged Files
=======================
File Name:
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archive
log/2007_11_08/o1_mf_1_3_3m5h1yby_.arc

using channel ORA_DISK_1

starting media recovery

archive log thread 1 sequence 2 is already on disk as file
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archive
log/2007_11_08/o1_mf_1_2_3m5h1svs_.arc
archive log thread 1 sequence 3 is already on disk as file
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archive
```

```
log/2007_11_08/o1_mf_1_3_3m5h1yby_.arc
archive log
filename=/oracle/product/10.2.0/db_1/flash_recovery_area/GDB
1/archivelog/2007_11_08/o1_mf_1_2_3m5h1svs_.arc thread=1
sequence=2
archive log
filename=/oracle/product/10.2.0/db_1/flash_recovery_area/GDB
1/archivelog/2007_11_08/o1_mf_1_3_3m5h1yby_.arc thread=1
sequence=3
media recovery complete, elapsed time: 00:00:01
Finished recover at 08-NOV-07

RMAN> alter database open resetlogs;

database opened
```

8. *Optional* - Create the *Net Service Name* and *Database Service Listener*:

To create a Net Service Name
Start Net Manager:

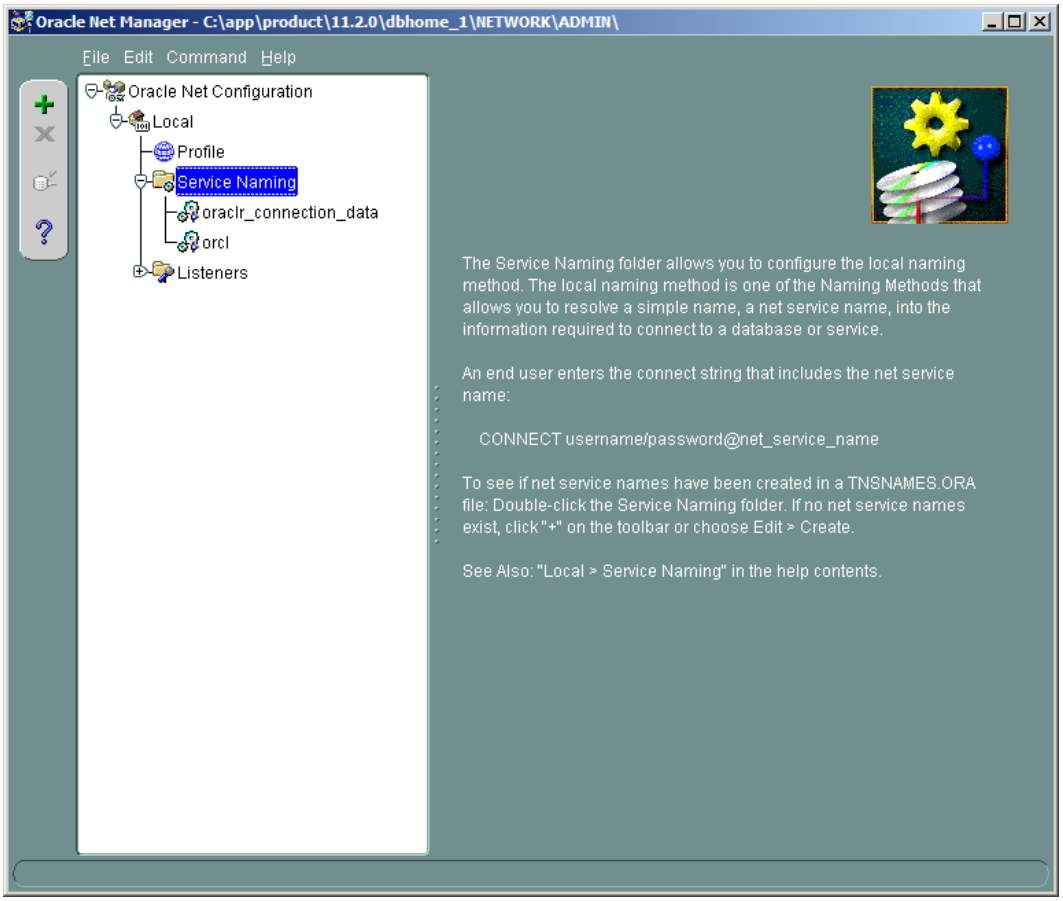
Windows
Click on the [Start Menu], select [Programs].

Select [Oracle - ${Home_Name}], in [Configuration and Migration Tools], choose [Net Manager].

Linux
Run netmgr from ${Oracle_Home}/bin:

```
netmgr
```

- Expand [Oracle Net Configuration], [Local].
- Select [Service Naming] and expand the sub tree on the left toolbar.


Oracle Net Manager - C:\app\product\11.2.0\dbhome_1\NETWORK\ADMIN\
File Edit Command Help
Oracle Net Configuration
Local
Profile
Service Naming
oraclr_connection_data
orcl
Listeners
The Service Naming folder allows you to configure the local naming method. The local naming method is one of the Naming Methods that allows you to resolve a simple name, a net service name, into the information required to connect to a database or service.
An end user enters the connect string that includes the net service name:
CONNECT username/password@net_service_name
To see if net service names have been created in a TNSNAMES.ORA file: Double-click the Service Naming folder. If no net service names exist, click "+" on the toolbar or choose Edit > Create.
See Also: "Local > Service Naming" in the help contents.

- The [Net Service Name] wizard will be launched to guide you through the procedure to create a net service name.

Net Service Name: Welcome
To access an Oracle database, or other service, across the network you use a net service name. This wizard will help you create a net service name.
Enter the name you want to use to access the database or service. It can be any name you choose.
Net Service Name:
Cancel
Back
Next

Note:
Ensure that the setting is saved afterward.

On the menu bar, click [File], then [Save Network Configuration].

To create a Database Service Listener
Start Net Manager:

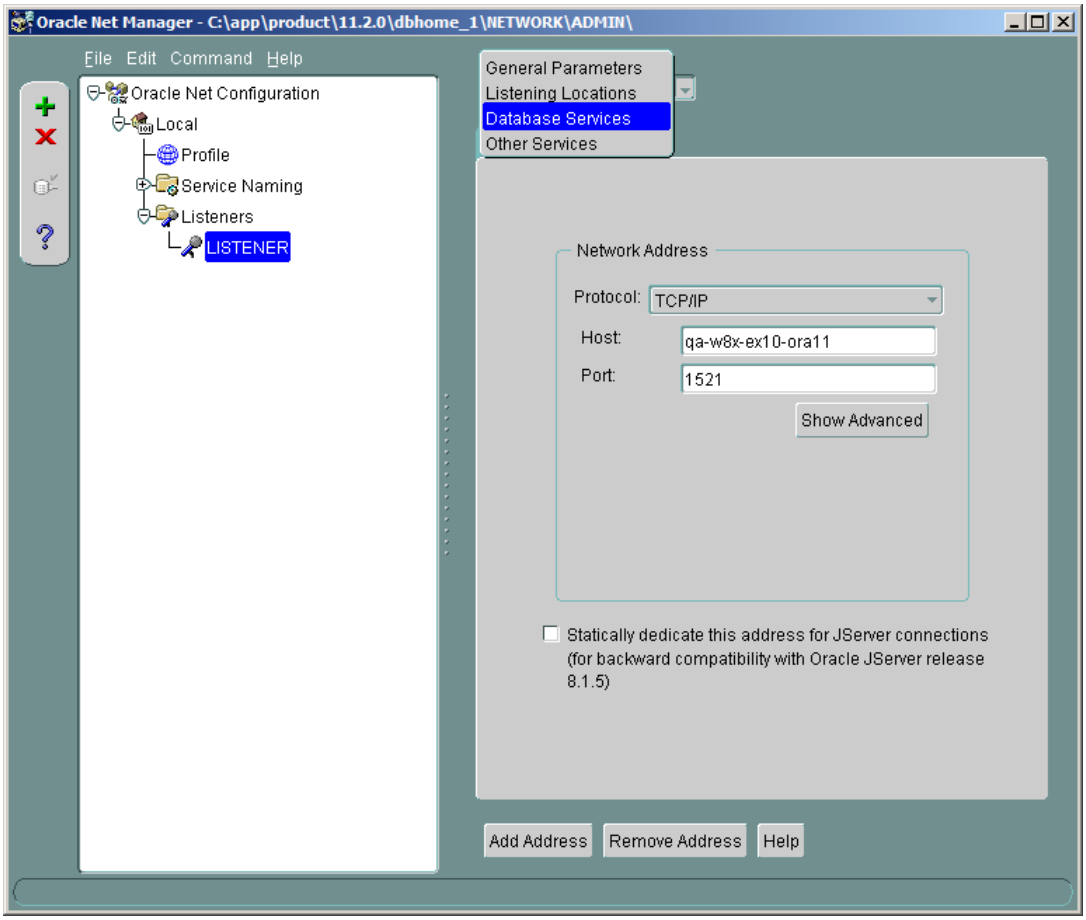
Windows
Click on the [Start Menu], select [Programs].

Select [Oracle - ${Home_Name}], in [Configuration and Migration Tools], choose [Net Manager]

Linux
Run netmgr from ${Oracle_Home}/bin:

```
netmgr
```

- Expand [Oracle Net Configuration], [Local].
- Under the [Listeners] sub tree, choose [LISTENER].
- Select [Database Services] from the combo box, then click [Add Database].



- Enter the *Global Database Name* and *SID*.

Note:
Ensure that the setting is saved afterward.

On the menu bar, click [File], then [Save Network Configuration]

17.7 How to restore individual tablespace

Restoring a tablespace required a backup of datafiles consistent with the existing archived logs and control files, as *REDO* will be applied during the restore operation.

Refer to the following instructions to restore tablespace of an Oracle database

1. Install OBM on the Oracle database server (if required).
2. Restore the Oracle database backup files from the OBS server.
3. Set *ORACLE_SID* to your database *System Identifier (SID)*.

```
Windows:
set ORACLE_SID=${database_SID}

Linux:
export ORACLE_SID=${database_SID}
```

4. Connect to database as *SYSDBA*.

```
sqlplus "/ as sysdba"
```

5. Shutdown the database.

```
SQL> shutdown immediate
```

6. Place the restored tablespace datafiles to the correct directory path.

   The Datafile name and path can be found by using the *REPORT SCHEMA* command:

   - Run *Oracle Recovery Manager (rman)* and connect to the target database.

```
rman target /
```

   - Start and mount database.

```
RMAN> startup mount
```

- List the names of all datafiles and tablespaces.

```
RMAN> report schema;
```

Example:

```
Report of database schema
File K-bytes    Tablespace  RB segs Datafile Name
---- ---------- ----------- ------- ------------------
1        419840 SYSTEM      ***
/oracle/OraHome1/oradata/GDB1/system01.dbf
2        204800 UNDOTBS1    ***
/oracle/OraHome1/oradata/GDB1/undotbs01.dbf
3         20480 CWMLITE     ***
/oracle/OraHome1/oradata/GDB1/cwmlite01.dbf
4         20480 DRSYS       ***
/oracle/OraHome1/oradata/GDB1/drsys01.dbf
5        141440 EXAMPLE     ***
/oracle/OraHome1/oradata/GDB1/example01.dbf
6         25600 INDX        ***
/oracle/OraHome1/oradata/GDB1/indx01.dbf
7         20480 ODM         ***
/oracle/OraHome1/oradata/GDB1/odm01.dbf
8         10240 TOOLS       ***
/oracle/OraHome1/oradata/GDB1/tools01.dbf
9         25600 USERS       ***
/oracle/OraHome1/oradata/GDB1/users01.dbf
10        39040 XDB         ***
/oracle/OraHome1/oradata/GDB1/xdb01.dbf
11            0 TS1         ***
/oracle/OraHome1/oradata/GDB1/TS1_datafile1.dbf
12            0 TS1         ***
/oracle/OraHome1/oradata/GDB1/TS1_datafile2.dbf
13            0 TS1         ***
/oracle/OraHome1/oradata/GDB1/TS1_datafile3.dbf
```

- Place all restored datafile that constitute the tablespace to the listed location.

For example with the data restored to /obm_restore:

```
/obm_restore/Oracle Database
Server/oracle/OraHome1/oradata/GDB1/TS1_datafile1.dbf

/obm_restore/Oracle Database
Server/oracle/OraHome1/oradata/GDB1/TS1_datafile2.dbf

/obm_restore/Oracle Database
Server/oracle/OraHome1/oradata/GDB1/TS1_datafile3.dbf
```

These files should be moved to:

```
/oracle/OraHome1/oradata/GDB1/TS1_datafile1.dbf

/oracle/OraHome1/oradata/GDB1/TS1_datafile2.dbf

/oracle/OraHome1/oradata/GDB1/TS1_datafile3.dbf
```

7. Restore tablespace.

```
RMAN> recover tablespace TS1;
```

Note:
The above command assumes that the tablespace name is TS1.

If the datafiles are consistent with the database, the following messages will be displayed:

Example:

```
RMAN> recover tablespace TS1;

Starting recover at 19-JUL-07
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=156 devtype=DISK

starting media recovery

archive log thread 1 sequence 1 is already on disk as file
D:\ORACLE\PRODUCT\10.
2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_19\O1_MF_1_1
_39Y98F0H_.ARC
archive log thread 1 sequence 2 is already on disk as file
D:\ORACLE\PRODUCT\10.
2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_19\O1_MF_1_2
_39Y98JSD_.ARC
archive log thread 1 sequence 3 is already on disk as file
D:\ORACLE\PRODUCT\10.
2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_19\O1_MF_1_3
_39Y9SW4D_.ARC
archive log
filename=D:\ORACLE\PRODUCT\10.2.0\FLASH_RECOVERY_AREA\GDB1\A
RCHIVELO
G\2007_07_19\O1_MF_1_1_39Y98F0H_.ARC thread=1 sequence=1
media recovery complete, elapsed time: 00:00:01
Finished recover at 19-JUL-07
```

If the datafiles are not consistent with the database, the following messages will be displayed:

Example:

```
RMAN> recover tablespace TS1;

Starting recover at 19-JUL-07
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=156 devtype=DISK
RMAN-00571:
===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS
===============
RMAN-00571:
===========================================================
RMAN-03002: failure of recover command at 07/20/2007
12:24:49
RMAN-06163: some datafiles cannot be recovered, aborting the
RECOVER command
RMAN-06166: datafile 7 cannot be recovered
RMAN-06166: datafile 6 cannot be recovered
RMAN-06166: datafile 5 cannot be recovered
```

In this event, please attempt the restore process again with a set of consistent datafiles.

The following error messages will be returned if there is archive log missing:

Example:

```
RMAN> recover tablespace TS1;

Starting recover at 20-JUL-07
using channel ORA_DISK_1

starting media recovery

archive log thread 1 sequence 12 is already on disk as file
D:\ORACLE\PRODUCT\10
.2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_18\O1_MF_1_
12_39VF4JNJ_.ARC
RMAN-00571:
===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS
===============
RMAN-00571:
===========================================================
RMAN-03002: failure of recover command at 07/20/2007
12:28:52
RMAN-06053: unable to perform media recovery because of
missing log
```

```
RMAN-06025: no backup of log thread 1 seq 13 lowscn 660617
found to restore
```

In this event, please attempt the restore process again after the missing archive log file is found.

8. Open database.

```
RMAN> alter database open;
```

Example:

```
$ export ORACLE_SID=GDB1

$ rman target /

Recovery Manager: Release 9.2.0.1.0 - Production

Copyright (c) 1995, 2002, Oracle Corporation.  All rights
reserved.

connected to target database (not started)

RMAN> startup mount

Oracle instance started
database mounted

Total System Global Area     235999352 bytes

Fixed Size                     450680 bytes
Variable Size                201326592 bytes
Database Buffers              33554432 bytes
Redo Buffers                    667648 bytes

RMAN> report schema;

using target database control file instead of recovery
catalog
Report of database schema

using target database controlfile instead of recovery
catalog
Report of database schema
File K-bytes    Tablespace           RB segs Datafile Name
---- ---------- ------------------- ------- ----------------
---
1        419840 SYSTEM              ***
/oracle/OraHome1/oradata/GDB1/system01.dbf
2        204800 UNDOTBS1            ***
/oracle/OraHome1/oradata/GDB1/undotbs01.dbf
```

```
3         20480 CWMLITE              ***
/oracle/OraHome1/oradata/GDB1/cwmlite01.dbf
4         20480 DRSYS                ***
/oracle/OraHome1/oradata/GDB1/drsys01.dbf
5        141440 EXAMPLE              ***
/oracle/OraHome1/oradata/GDB1/example01.dbf
6         25600 INDX                 ***
/oracle/OraHome1/oradata/GDB1/indx01.dbf
7         20480 ODM                  ***
/oracle/OraHome1/oradata/GDB1/odm01.dbf
8         10240 TOOLS                ***
/oracle/OraHome1/oradata/GDB1/tools01.dbf
9         25600 USERS                ***
/oracle/OraHome1/oradata/GDB1/users01.dbf
10        39040 XDB                  ***
/oracle/OraHome1/oradata/GDB1/xdb01.dbf
11            0 TS1                  ***
/oracle/OraHome1/oradata/GDB1/TS1_datafile1.dbf
12            0 TS1                  ***
/oracle/OraHome1/oradata/GDB1/TS1_datafile2.dbf
13            0 TS1                  ***
/oracle/OraHome1/oradata/GDB1/TS1_datafile3.dbf

List of Temporary Files
=======================
File Size(MB) Tablespace           Maxsize(MB) Tempfile Name
---- -------- -------------------- ----------- -------------
-------
1    20       TEMP                 32767
D:\ORACLE\PRODUCT\10.2.0\ORADATA\
GDB1\TEMP01.DBF

RMAN> recover tablespace TS1;

Starting recover at 30-AUG-07
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=11 devtype=DISK

starting media recovery
media recovery complete

Finished recover at 30-AUG-07

RMAN> alter database open;

database opened
```

17.8 Export and Import a database (logical backup)

For logical database backup and recovery, one can also utilize Oracle's built-in export / import utilities.

When exporting, database objects are dumped to a binary file which can then be imported into another Oracle database (e.g. database migration).

Note:
Data exported are in proprietary binary file format; therefore, they can only be used between Oracle databases. One cannot export data and expect to import it into a non-Oracle database.

Refer to the following instructions to perform a logical backup (export):
For example to export the database -

1. Export the database to a dump file with the following command.

```
exp username/password FULL=y FILE='/export-
destination/data.dmp' LOG='/log-destination/export.log'
```

Example:

```
$ exp system/pwd123 FULL=y FILE='/oracle/data.dmp'
LOG='/oracle/export.log'

Connected to: Oracle Database 10g Enterprise Edition Release
10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options
Export done in WE8MSWIN1252 character set and AL16UTF16
NCHAR character set

About to export the entire database ...
. exporting tablespace definitions
. exporting profiles
. exporting user definitions
. exporting roles
. exporting resource costs

                          //////////////////////
                          // ... exporting ... //
                          //////////////////////

. exporting dimensions
. exporting post-schema procedural objects and actions
. exporting user history table
. exporting default and system auditing options
. exporting statistics
Export terminated successfully without warnings.
```

2. Backup the exported dump file to OBS.

   Create a file type backup set to backup the newly exported dump file to an off-site server.

   Note:
   For more details, please refer to the File Backup chapter of this same guide.

Refer to the following instructions to perform a logical restore (import):
For example to import a database -

1. Restore the exported dump file from OBS.

2. Import the database with the following command.

```
imp username/password FULL=y FILE='/import-
source/data.dmp' LOG='/log-destination/import.log'
```

Example:

```
$ imp system/pwd123 FULL=y FILE='/oracle/data.dmp'
LOG='/oracle/import.log'

Connected to: Oracle Database 10g Enterprise Edition Release
10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

Export file created by EXPORT:V10.02.01 via conventional
path
import done in WE8MSWIN1252 character set and AL16UTF16
NCHAR character set
. importing SYSTEM's objects into SYSTEM
. importing OLAPSYS's objects into OLAPSYS
. importing SYSMAN's objects into SYSMAN
. importing SYSTEM's objects into SYSTEM
. importing OLAPSYS's objects into OLAPSYS

            //////////////////////
            // ... importing ... //
            //////////////////////

. importing OLAPSYS's objects into OLAPSYS
. importing SYSTEM's objects into SYSTEM
. importing OLAPSYS's objects into OLAPSYS
. importing SYSMAN's objects into SYSMAN
. importing SCOTT's objects into SCOTT
Import terminated successfully without warnings.
```

18 Backup / Restore Microsoft SQL Server

This chapter describes how to backup and restore Microsoft SQL Server with OBM.

18.1 Supported versions

The MS SQL Database backup module is supported for the following SQL Server versions:

- MS SQL 2000
- MS SQL 2005
- MS SQL 2008 / R2

For more details, please refer to Help Centre Article:
https://help..com/openArticle.aspx?aid=2323

18.2 Requirements and recommendations

OBM can be installed on the SQL server, or a separate backup client machine.

For OBM installation on the SQL Server
Please ensure that the following requirements are met by the SQL Server:

1. OBM version 5.5.8.0 or above is installed on the SQL server.

   Note:
   MS SQL 2008 R2 is only supported for OBM version 5.5.8.0 or above.

2. Databases files are spooled to a temporary directory before being uploaded to the offsite backup server.

   It is recommended that the temporary directory have disk space of at least 120% of the total database size.

3. It is recommended that the temporary directory be configured on a local drive.

4. The SQL Windows service must have read write permission to the temporary directory.

5. For database with simple recovery model, only full database and differential database backups are allowed.

   To perform a transaction log backup, please change the corresponding databases' recovery model from simple to full.

For OBM installation on a separate Backup Client Machine

Please ensure that the following requirements are met by the Backup Client Machine:

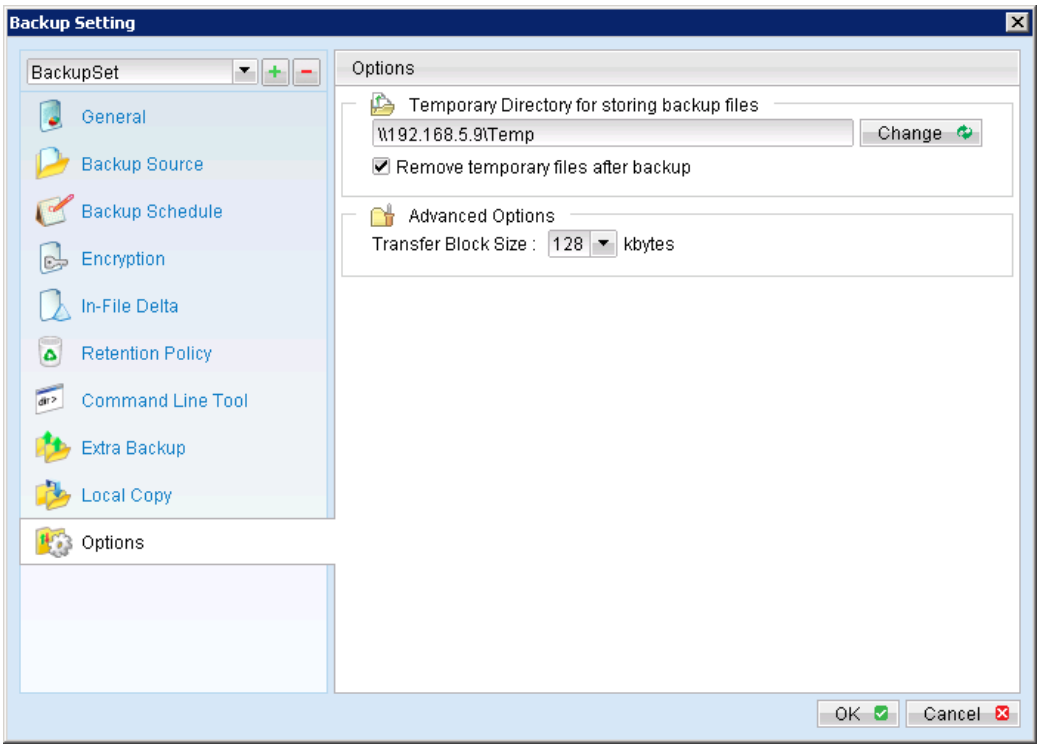
1. OBM version 5.5.8.0 or above is installed on the dedicated machine for backup.

   Note:
   MS SQL 2008 R2 is only supported for OBM version 5.5.8.0 or above.

2. Databases files are spooled to the temporary directory before being uploaded to the offsite backup server.

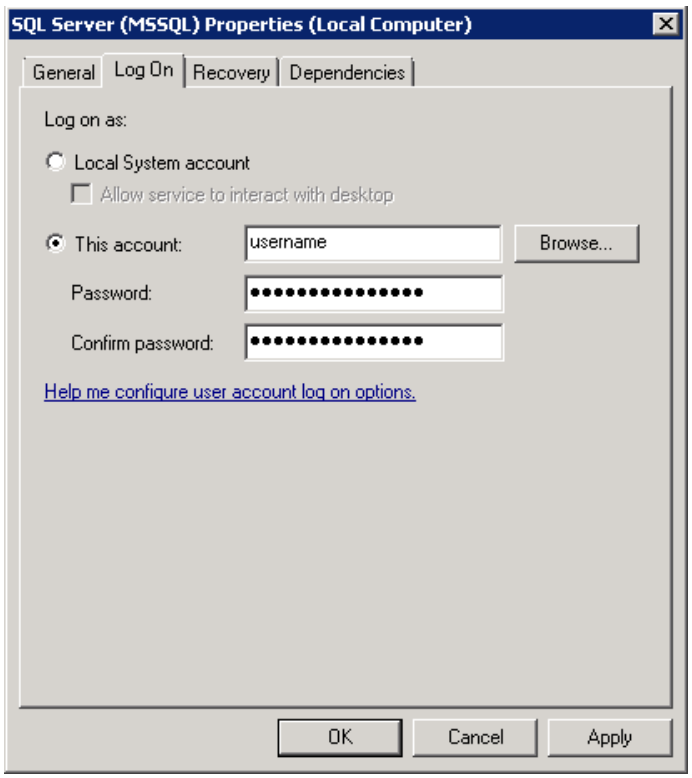
   It is recommended that the temporary directory have disk space of at least 120% of the total database size.

3. Since OBM is not installed directly on the SQL server, the temporary directory configured for the backup set must be a network path that is accessible by the SQL server.



4. The SQL Windows service must have read write permission to the network temporary directory.

   Please update the service's [Log On] setting of the services if required.



5. For database with simple recovery model, only full database and differential database backups are allowed.

   To perform a transaction log backup, please change the corresponding databases' recovery model from simple to full.

Considerations for backup and restore of system databases

Refer to the following tables for considerations for backup and restore of system databases:

Considerations for backup of system databases:

SQL server maintains a set of system level database which are essential for the operation of the server instance.

Several of the system databases must be backed up after every significant update, they includes:

- master
- model
- msdb

For SQL database with replication enabled.

- distribution

This table summarizes all of the system databases.

System database	Description	Backup required	Suggestion
master	The database that records all of the system level information of a SQL server system.	Yes	Back up the master database as often as necessary to protect the data sufficiently for your business needs. Microsoft recommends a regular backup schedule, which you can supplement with manual backup after any substantial update.
model	The template for all databases that are created on the instance of SQL server.	Yes	Backup the model database only when necessary, for example, after customizing its database options. Microsoft recommends that you create only full database backups of model, as required. Because model is small and rarely changes, backing up the log is unnecessary.
msdb	The msdb database is used by SQL Server Agent for scheduling alerts and jobs, and for recording operators. It also contains history tables (e.g. backup / restore history table).	Yes	Back up msdb whenever it is updated.
tempdb	A workspace for holding temporary or intermediate result sets. This database is recreated every time an	No	The tempdb system database cannot be backed up.

	instance of SQL server is started.		
distribution	The distribution database exists only if the server is configured as a replication distributor. It stores metadata and history data for all types of replication, and transactions for transactional replication.	Yes	Replicated databases and their associated system databases should be backed up regularly.

Considerations for restore of system databases:

System database	**Restore suggestion**
master	To restore any database, the instance of SQL server must be running. Startup of an instance of SQL server requires that the master database is accessible and at least party useable. Restore or rebuild the master database completely if master becomes un-useable.
model	Restore the model database if: • The master database has been rebuilt. • The model database has been damaged, for example due to media failure. • The model database has been modified, in this case, it is necessary to restore model from a backup when you rebuild master, because the Rebuild Master utility deletes and recreates model.
msdb	Restore the msdb database if:

	• The master database has been rebuilt.
distribution	For restore strategies of distribution database, please refer to the following online document from Microsoft for more details: http://msdn.microsoft.com/en-us/library/ms152560.aspx

18.3 Overview

The following steps are performed during a backup job:

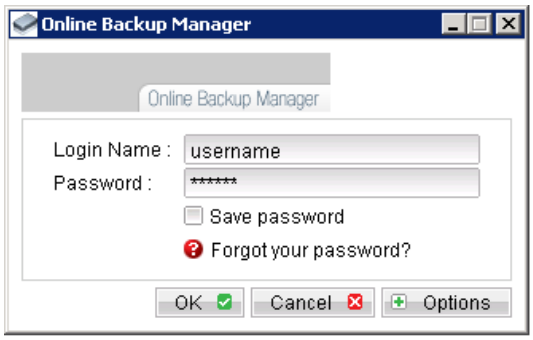
1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Connection to the SQL server is established.
4. Commands are issued for the database or transaction log backup files to be spooled to the temporary spool path.
5. Server and local file lists are compared to determine which file will be uploaded.
6. Delta file is generated for modified file (if necessary).
7. Data are encrypted, compressed, and uploaded to the backup server.
8. Data are removed from the temporary spool path.
9. Backup completed successfully.

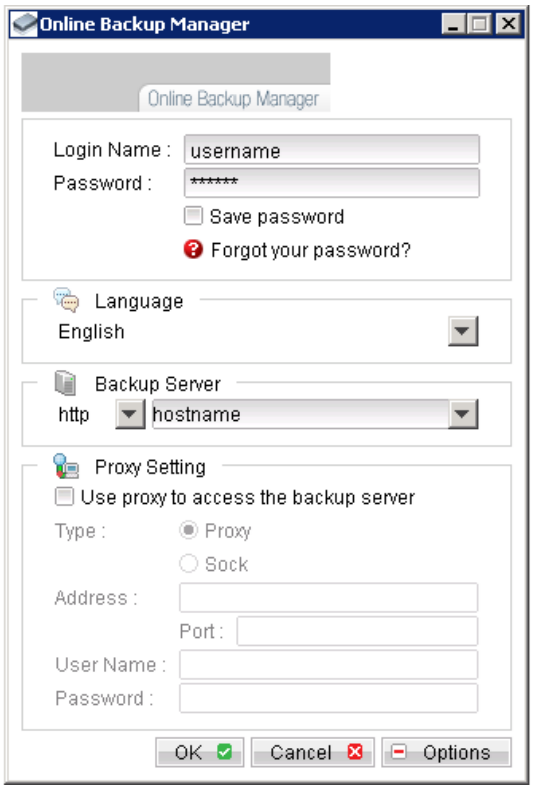
18.4 How to backup Microsoft SQL Server database

Refer to the following instructions to backup Microsoft SQL Server database:

1. Login to the backup application's user interface.

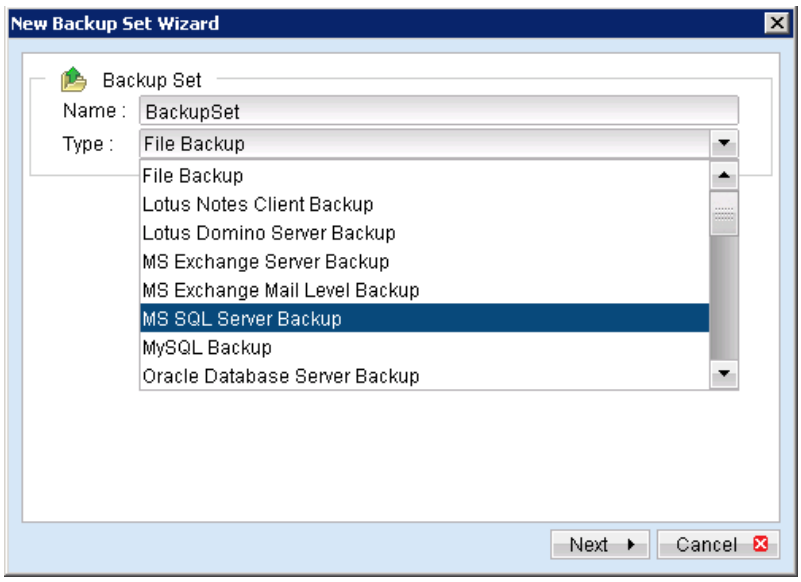
   Double-click on the OBM desktop icon or right-click on the system tray icon:



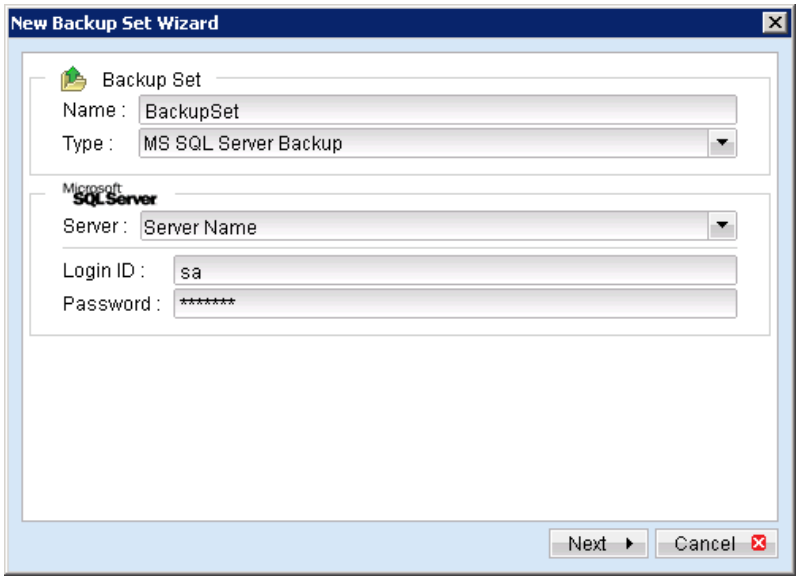


2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

3. Create a MS SQL Server Backup set by selecting [MS SQL Server Backup] from the backup set type dropdown menu.



4. Enter the corresponding information required:

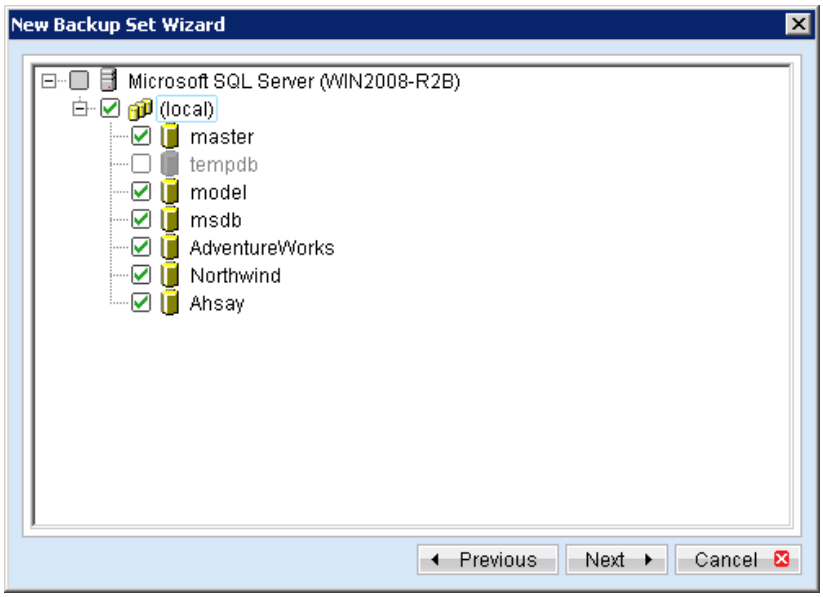


Menu Items	Description
Name	Enter a backup set name of your choice.
Type	Select backup set type [MS SQL Server Backup].
Server	Select the server instance to be backed up.
Login ID	Enter the Login ID of the MS SQL administrator account. (Only for SQL Server database set to SQL Server and Windows Authentication mode)
Password	Enter the password of the MS SQL administrator account. (Only for SQL Server database set to SQL Server and

	Windows Authentication mode)

5. Select [Next] to proceed.

6. Select the corresponding database for backup.



7. Configure a backup schedule for unattended backups.

   Note:
   Multiple backup schedules of different types can be configured for the same backup set.

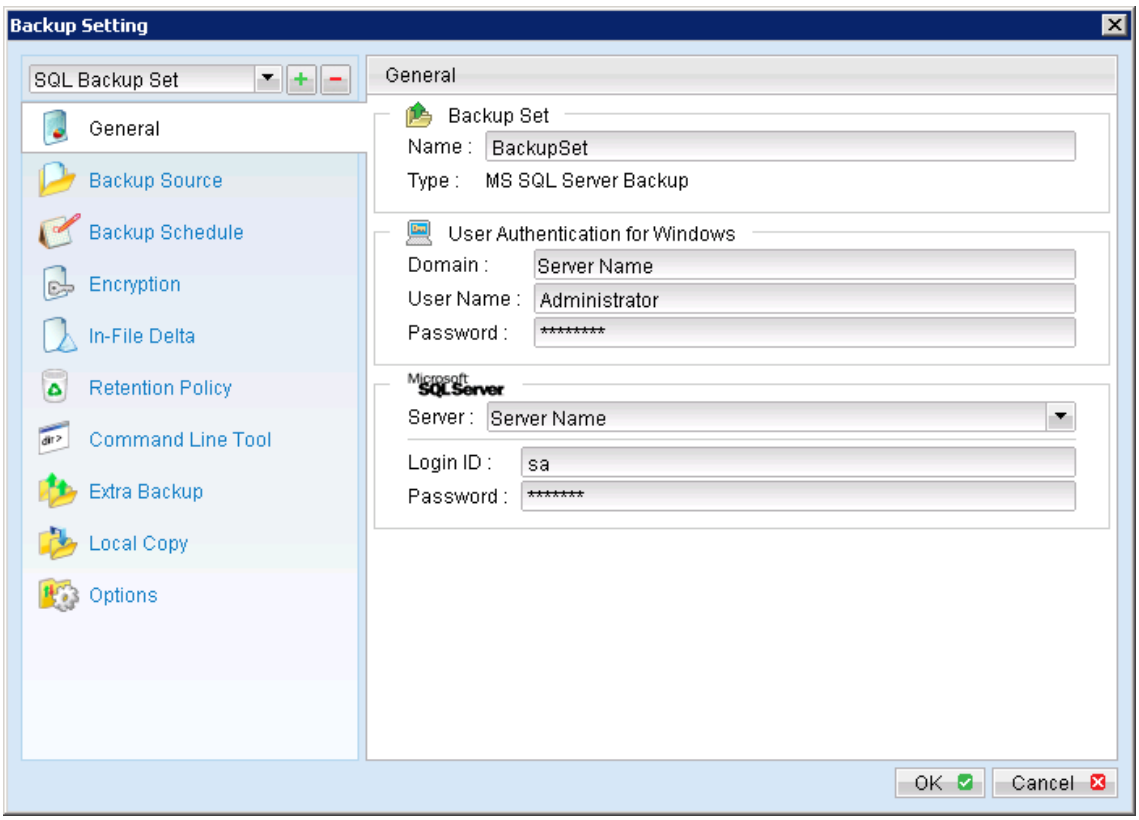
8. Select an encryption setting for your backup set.

9. Press the [OK] button to complete the configuration of backup set.

10. For SQL Server database with Windows Authentication mode:

    Configure the [User Authentication for Windows] setting.

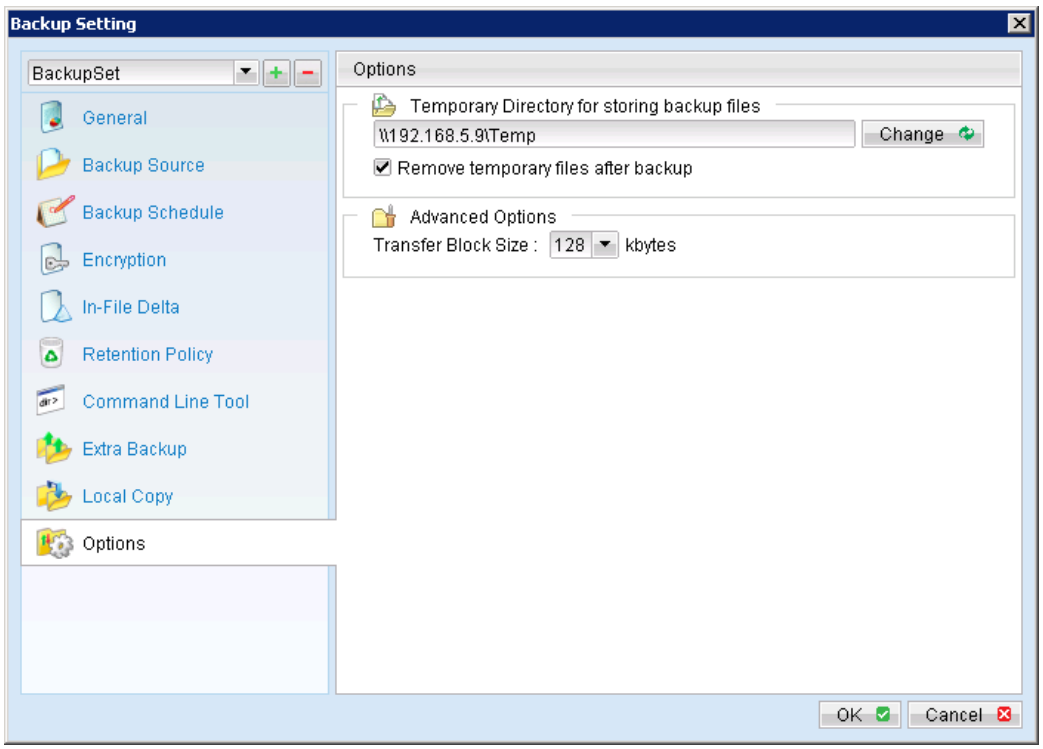
    Enter the login credentials of a Windows account with sufficient permission to access the MS SQL databases server.



Menu Items	Description
Domain	SQL server under a domain: Enter the name of the domain which the MS SQL server reside in. SQL server under a workgroup: Enter the computer name of the MS SQL server
User Name	Enter the username of the SQL administrator Windows account.
Password	Enter the username of the SQL administrator Windows account.

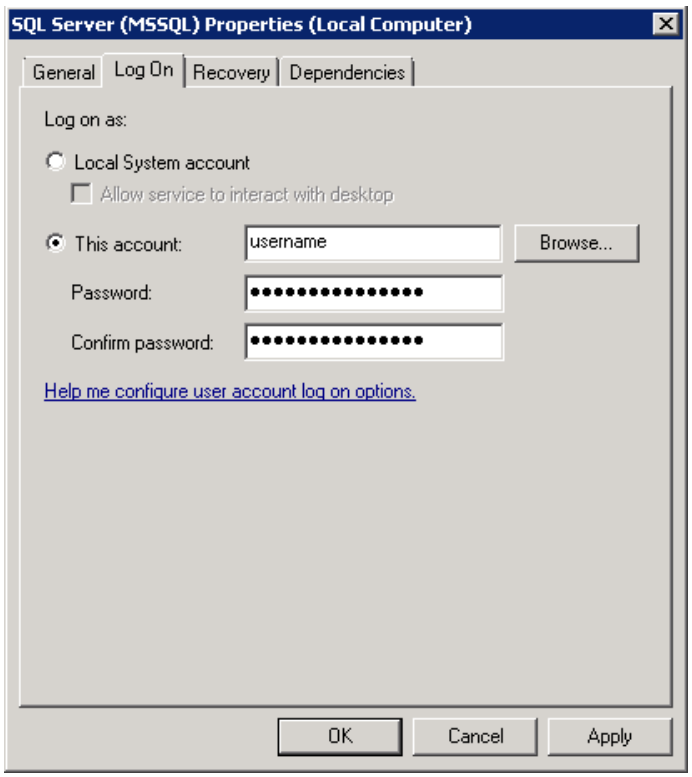
11. For OBM not installed on the MS SQL Server:

    Configure the temporary directory to a network path that is accessible by the SQL database server.



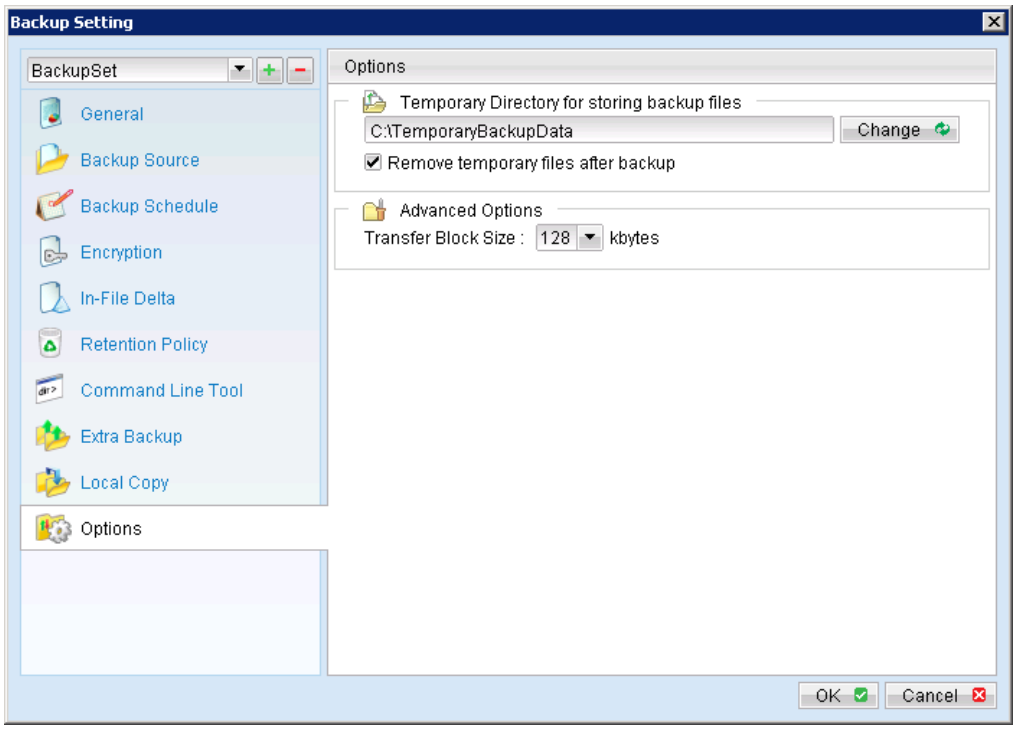
Important:
Please ensure that the MS SQL Server's SQL Windows service has read write permission to the network temporary directory.

Please update the service's [Log On] setting of the services if required.



12. For OBM installed on the MS SQL server:

    Configure the temporary directory to a local, USB or network path.

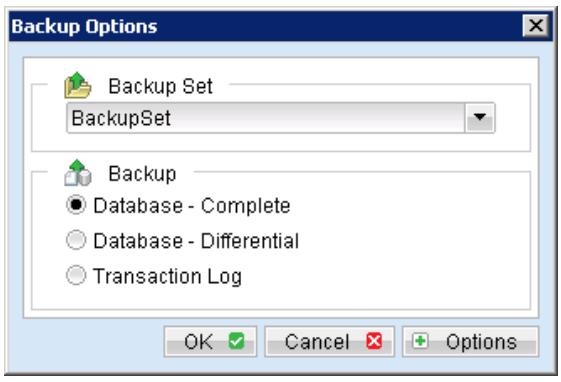


Important:
Please ensure that the MS SQL Server's SQL Windows service has read write permission to the network temporary directory.

13. Scheduled backup will run automatically at the configured schedule time.

14. Click [Backup] button on the left panel to perform a backup immediately.

15. Select the backup type to be performed:



Menu Items	Description
Database - Complete	Perform a complete database backup.
Database - Differential	Perform a differential database backup.

Transaction Log	Perform a transaction log backup.

18.5 How to restore Microsoft SQL Server database

Refer to the following instructions to restore Microsoft SQL Server database:

1. Prepare the operating system for the MS SQL Server restore (if required).

   Install the original version of Windows and SQL Server (with the same level of service pack installed as in the original system).

2. Ensure that all SQL related Windows services are up and running.

3. Install OBM (if required).

4. Restore the SQL databases from backup; restore the database backup files from the OBS server.

5. Continue with the following steps to restore the system database and the user databases.

   Important:
   It is not necessary to restore the system databases for user database recovery.

   Please refer to the requirements and recommendations (considerations for backup and restore of system databases) section in the above for details.

18.5.1 Restore Microsoft SQL Server 2000 database

18.5.1.1 Restore master database

Refer to the following instructions to restore the master database:

1. Stop the SQL instance.
2. Restart the SQL instance in single-user mode.

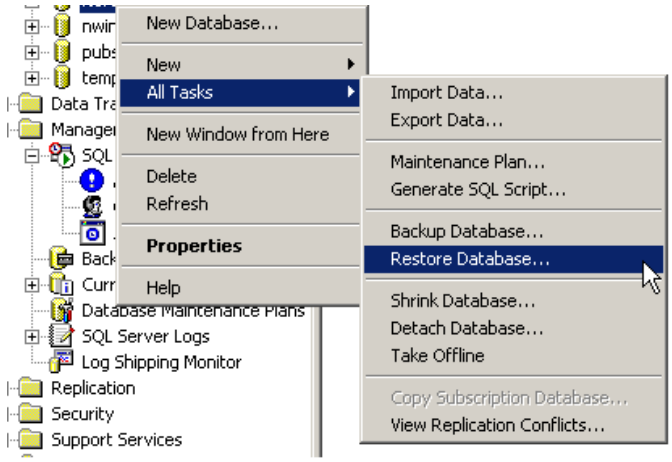
   From a command prompt, browse to the appropriate directory for the instance of SQL to start

   Enter the following command.

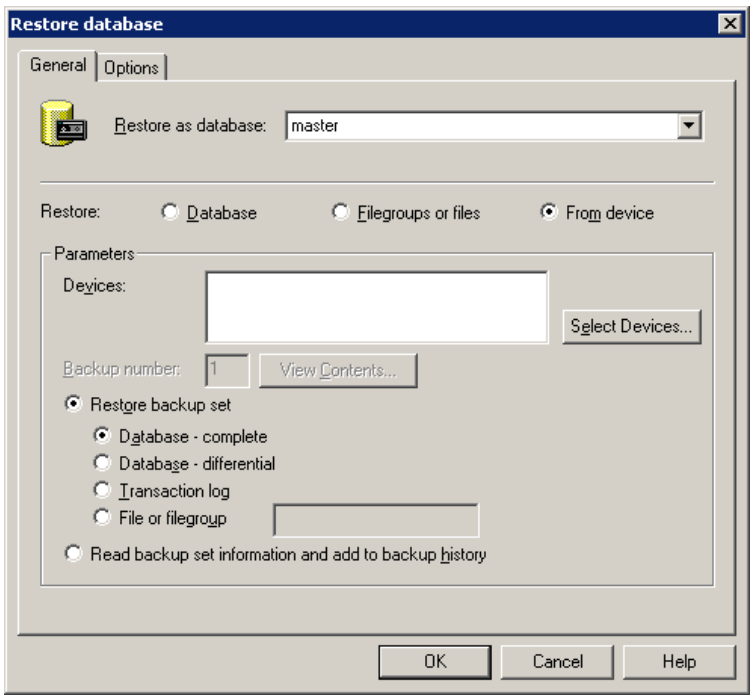
```
For default instance

>sqlservr.exe -c -m


For named instance

>sqlservr.exe -c -m {instance_name}
```

Important
Only perform Step 1 and 2 if you are restoring the master database.

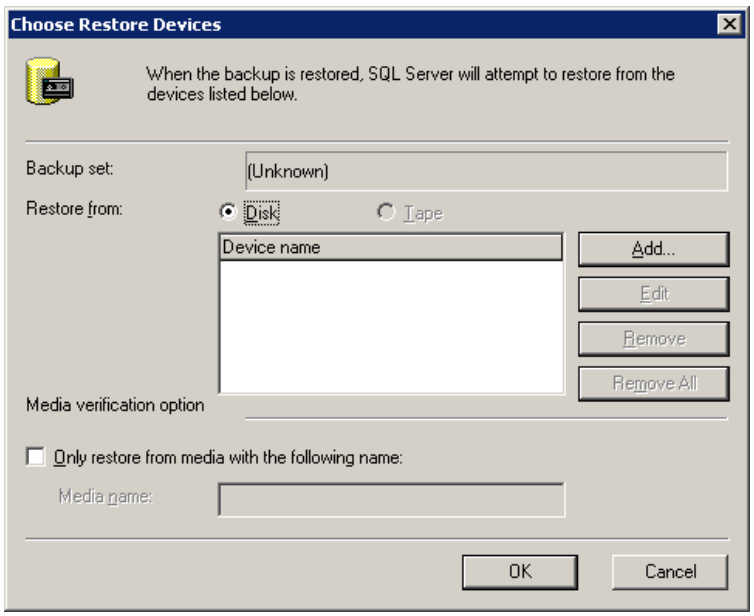
3. Open SQL Server Enterprise Manager; connect to the server where the backup is to be restored.
4. Right click the master database and select [All Tasks], then select [Restore database].



5. Select the [From device] radio button and [Select Devices].

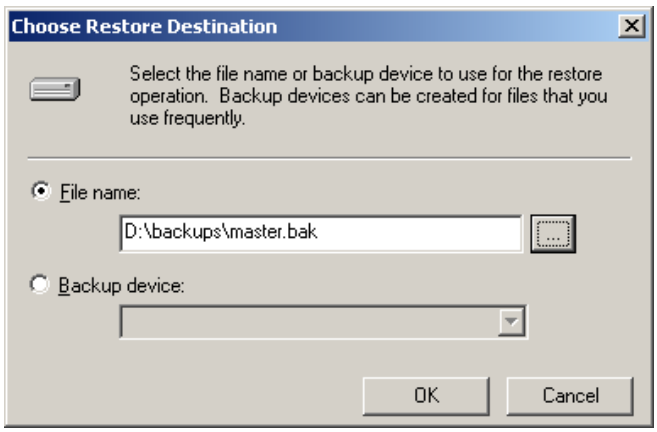


6. In the [Choose Restore Devices] dialog box, select the [Disk] radio button.



7. Click the [Add] button to display the dialog box, enter the file name of the backup file (restored from OBS) that is to be restored.

   If the file exists on a network share, provide the UNC share name in the File name text box.


Choose Restore Destination
Select the file name or backup device to use for the restore operation. Backup devices can be created for files that you use frequently.
File name:
D:\backups\master.bak
Backup device:
OK
Cancel

8. Click the Options tab and select appropriate options for the restore operation.

9. Click OK in the Restore Database dialog box to begin the restore process.

10. Restart the SQL instance in multi-user mode afterward.

    Restart the SQL Windows services, or enter the following command.

```
For default instance

>sqlservr.exe -c


For named instance

>sqlservr.exe -c {instance_name}
```

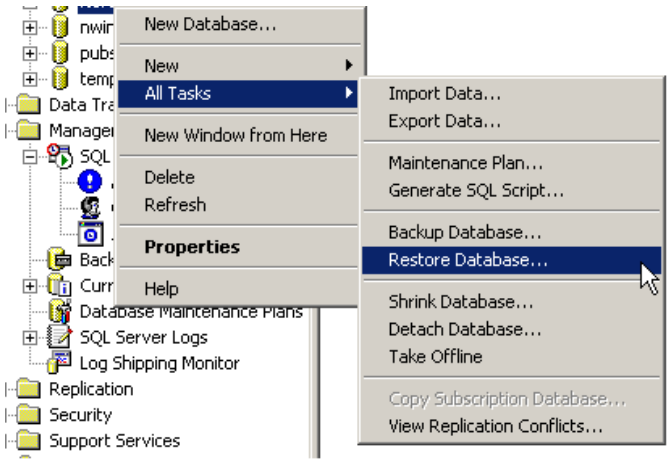
11. Continue with the following steps to restore other system database and the user databases.

18.5.2.1 Restore other system or user database (complete backup)

Refer to the following instructions to restore a complete backup:

1. Open SQL Server Enterprise Manager; connect to the server where the backup is to be restored.

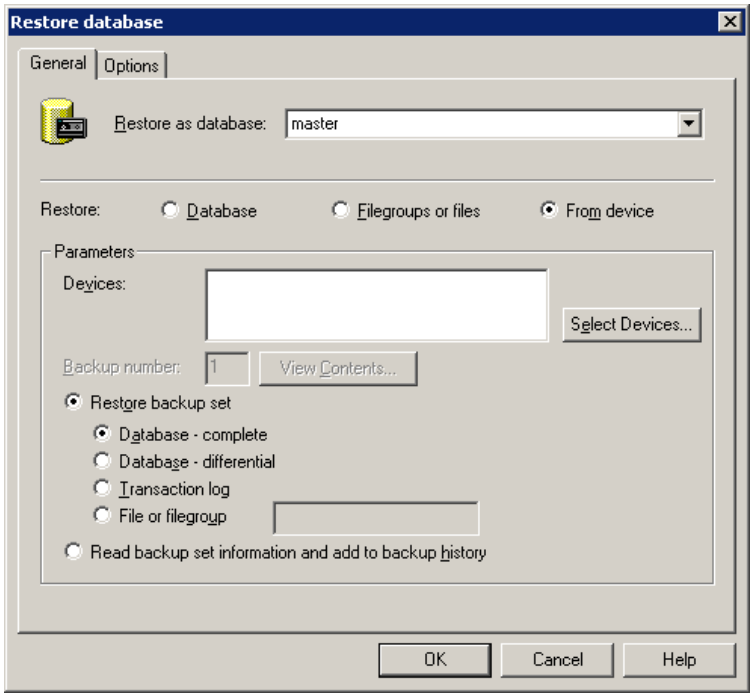
2. Right click the corresponding database and select [All Tasks], then select [Restore database].



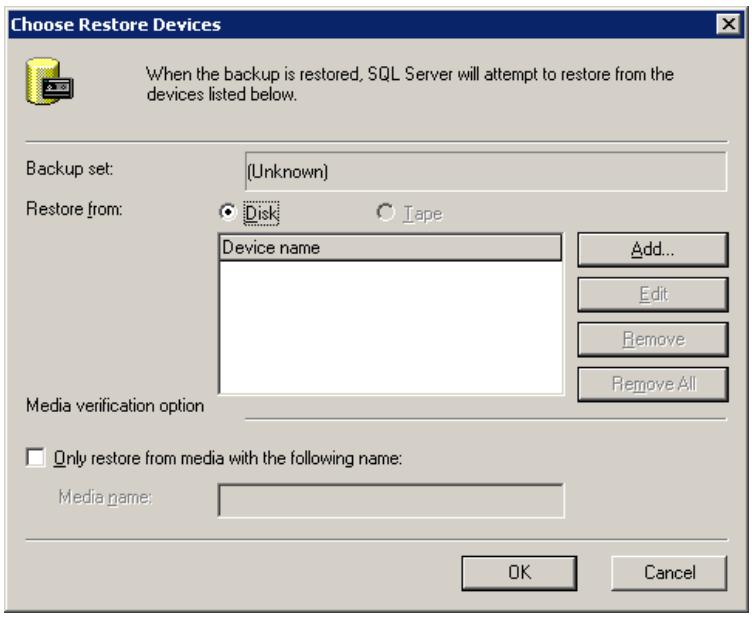
Note:
SQL Server databases may be backed up on one server and restored to another server.

If the target database does not exist on the server, right click on any database instead. A new database can be created while restoring the backup.

3. Select the [From device] radio button and [Select Devices].

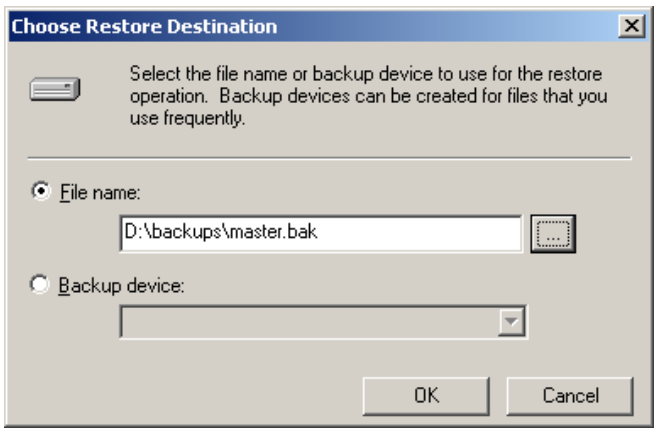


4. In the [Choose Restore Devices] dialog box, select the [Disk] radio button.

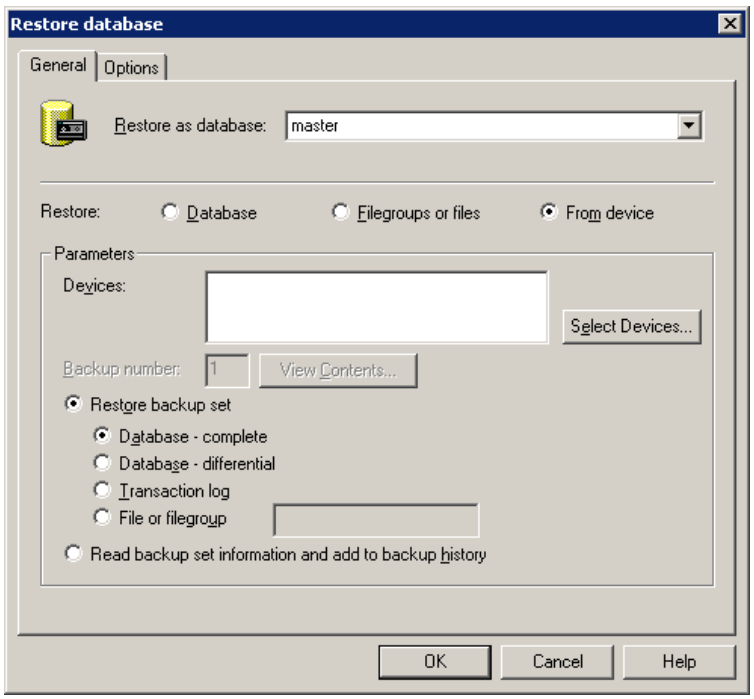


5. Click the [Add] button to display the dialog box, enter the file name of the backup file (restored from OBS) that is to be restored.

   If the file exists on a network share, provide the UNC share name in the File name text box.

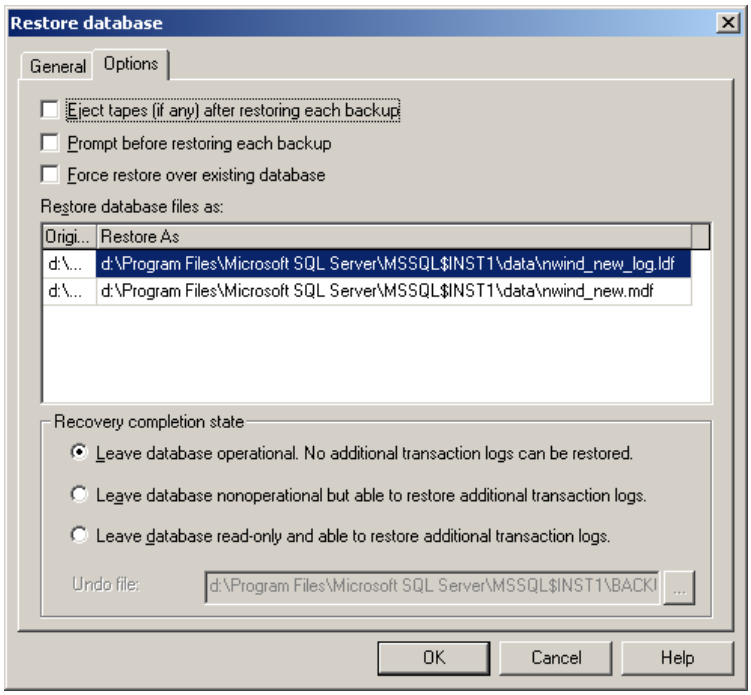

Choose Restore Destination
Select the file name or backup device to use for the restore operation. Backup devices can be created for files that you use frequently.
File name:
D:\backups\master.bak
...
Backup device:
OK
Cancel

6. Select the [Restore backup set] radio button, and [Database - complete].



7. Click the Options tab and select appropriate options for the restore operation.

   For the [Recovery completion state] setting:



Important:
If this is the final backup to be restored, select -

[Leave database operational. No additional transaction logs can be restored]

If there are further differential or transaction log to be applied, selection one of the other two options for the Recovery completion state

8. To start the restore operation, click OK.

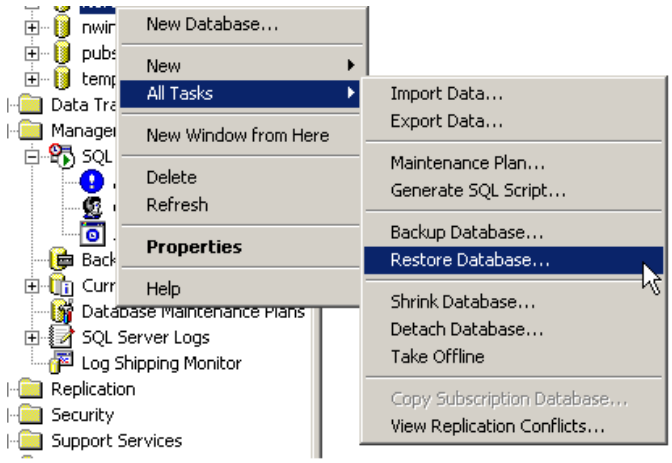
9. Continue to the next section to restore differential or transaction log backup.

18.5.3.1 Restore other system or user database (differential / transaction log backup)

Refer to the following instructions to restore a differential or transaction log backup:

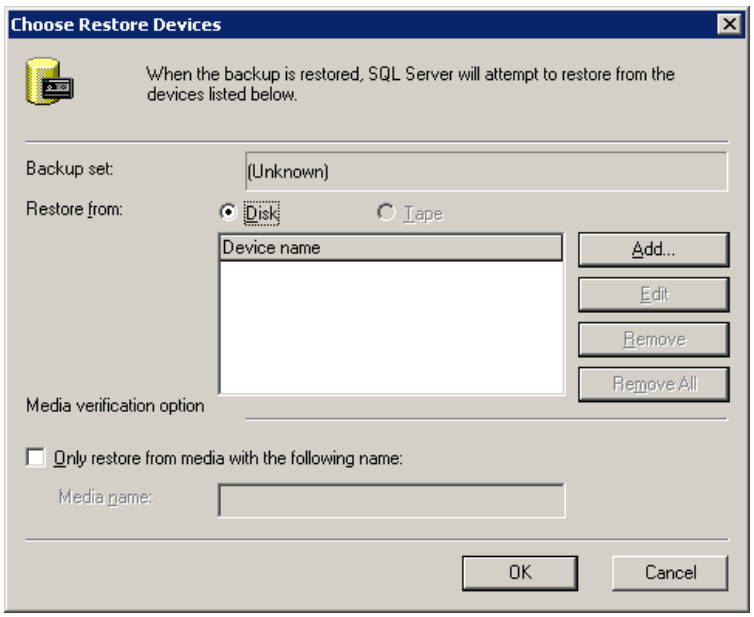
1. Open SQL Server Enterprise Manager.

2. Right click the corresponding database, select [All Tasks], and then select [Restore database].

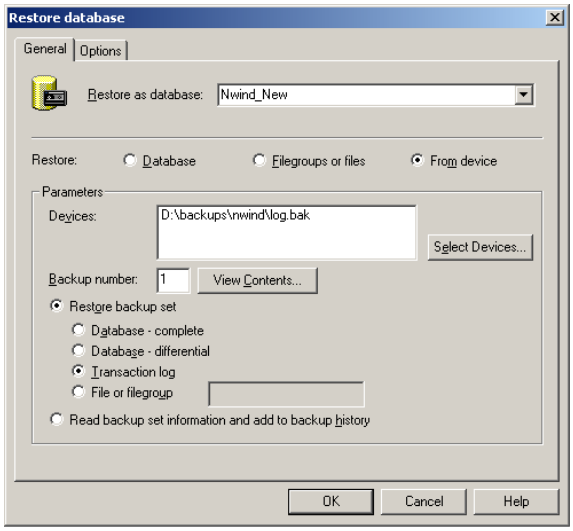


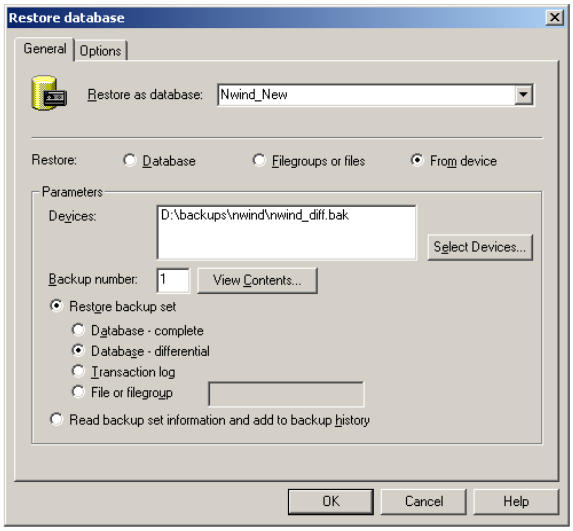
3. In the window that is displayed, select the [From device] option.

4. Add the backup device (restored from OBS), refer to the procedure explained in previous section.



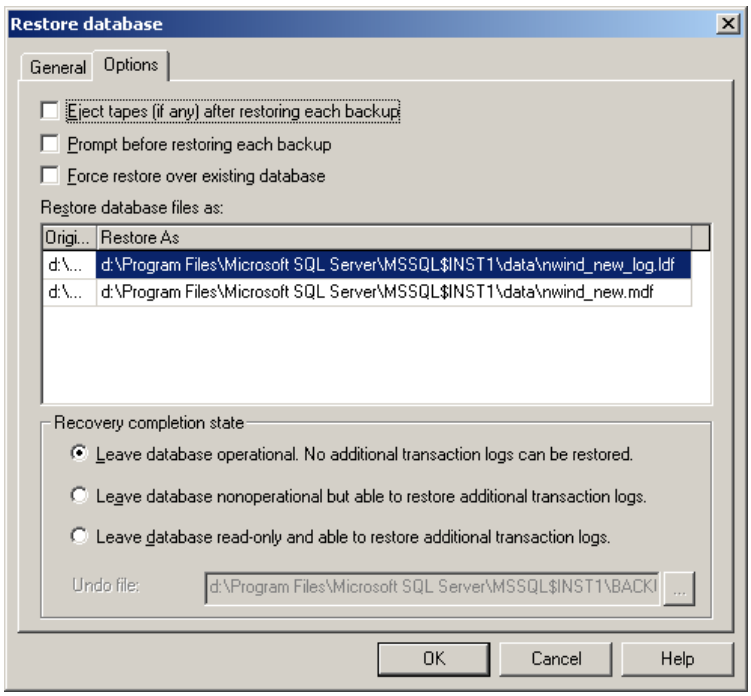
5. Select [Database - differential] or [Transaction log] according to the backup file you are restoring.





6. Click the Options tab and select appropriate options for the restore operation.

   For the [Recovery completion state] setting:



Important:
If this is the final transaction log to be applied, select -

[Leave database operational. No additional transaction logs can be restored]

If there are further backups to be applied afterward, one of the other two options for the Recovery completion state.

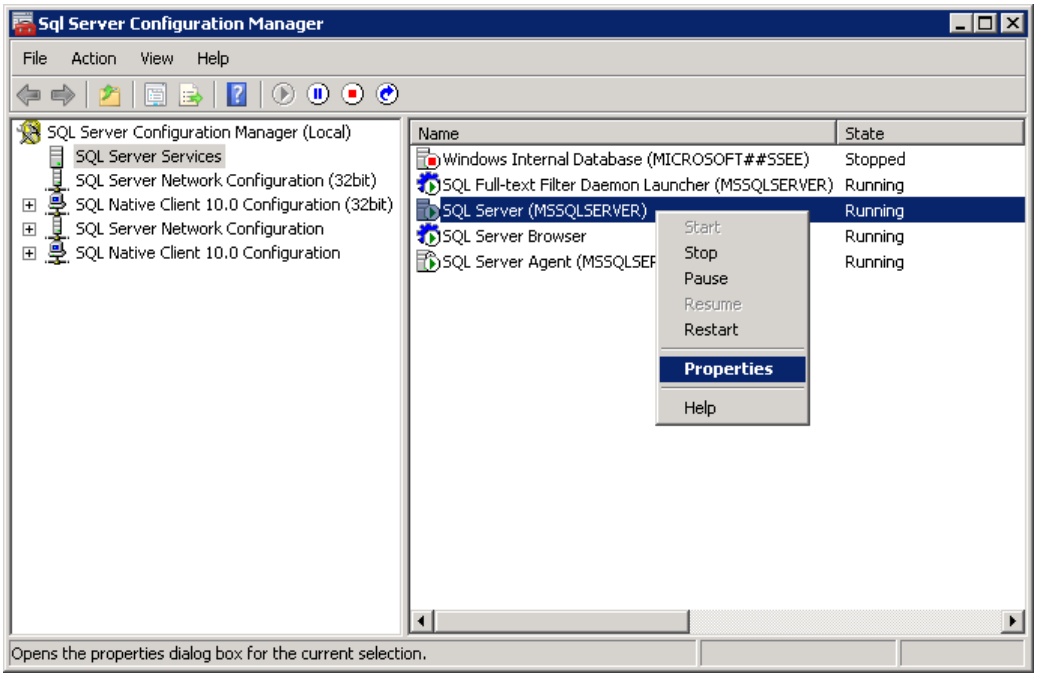
7. To start the restore operation, click OK.

18.5.2 Restore Microsoft SQL Server 2005 / 2008 database

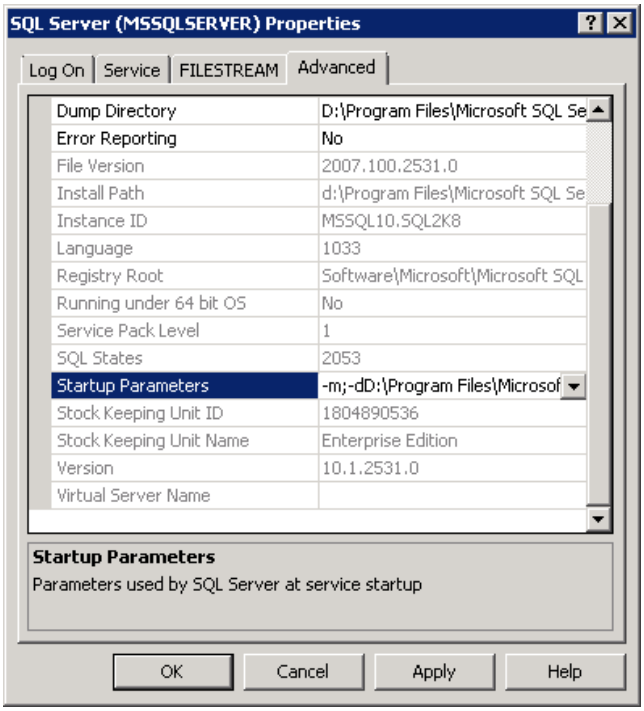
18.5.1.2 Restore master database

Refer to the following instructions to restore the master database:

1. Stop the SQL instance.
2. Restart the SQL instance in single-user mode.
   - In SQL Server Configuration Manager, click [SQL Server Services].
   - In the right pane, right-click SQL Server, and then click [Properties].



- On the Advanced tab, in the Startup Parameters box, type the parameters -m separated by semicolons.



- Restore the database engine afterward.

Important:
When you start SQL Server in single-user mode, first stop SQL Server Agent.

Otherwise, SQL Server Agent might connect first, preventing you from connecting as a second user.

3. To restore a full database backup of master, use the following *RESTORE DATABASE Transact-SQL* statement:

```
>RESTORE DATABASE master FROM ${backup_device} WITH
REPLACE
```

${backup_device} is the database file restored from OBS:

```
C:\>sqlcmd

1>RESTORE DATABASE master FROM DISK = 'C:\temp\master.bak'
WITH REPLACE;

2>GO
```

4. After master is restored, the instance of SQL Server shuts down and terminates the *sqlcmd* process.

   Before you restart the server instance, ensure to remove the single user startup parameter that you have added previously in Step 2.

5. Restart the server instance and continue other recovery steps such as restoring other databases.

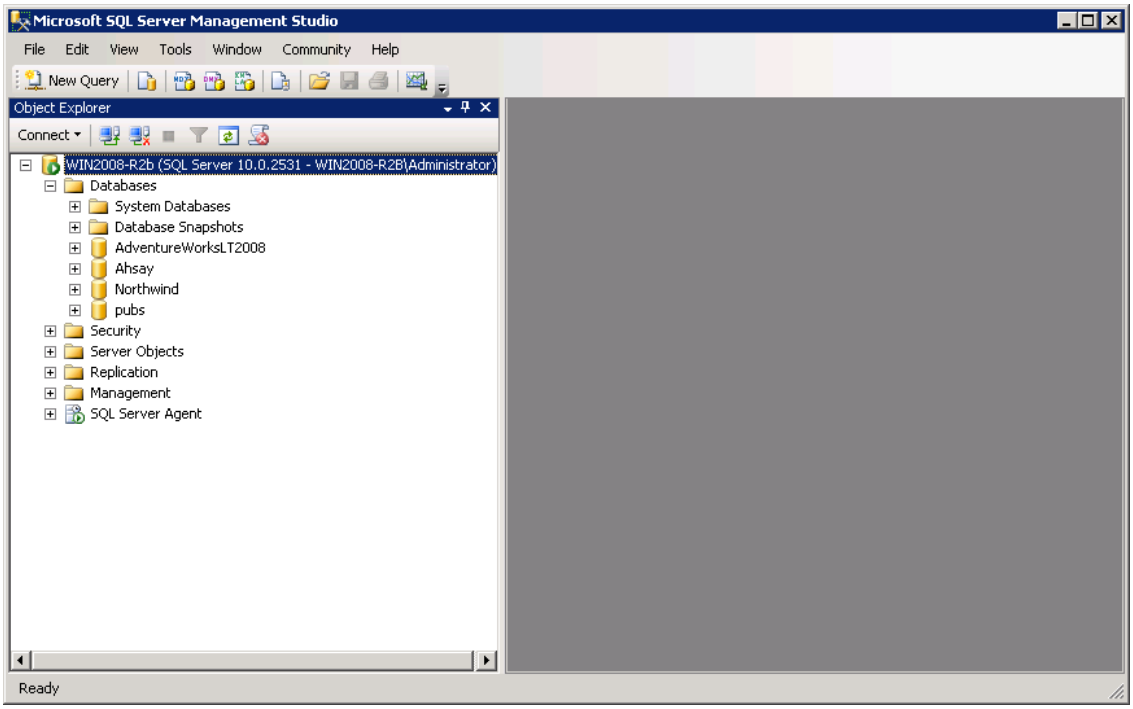
18.5.2.2 Restore other system or user database (complete backup)

Refer to the following instructions to restore a complete backup:

1. Open SQL Server Management Studio; connect to the server where the backup is to be restored.

2. Expand [Databases].

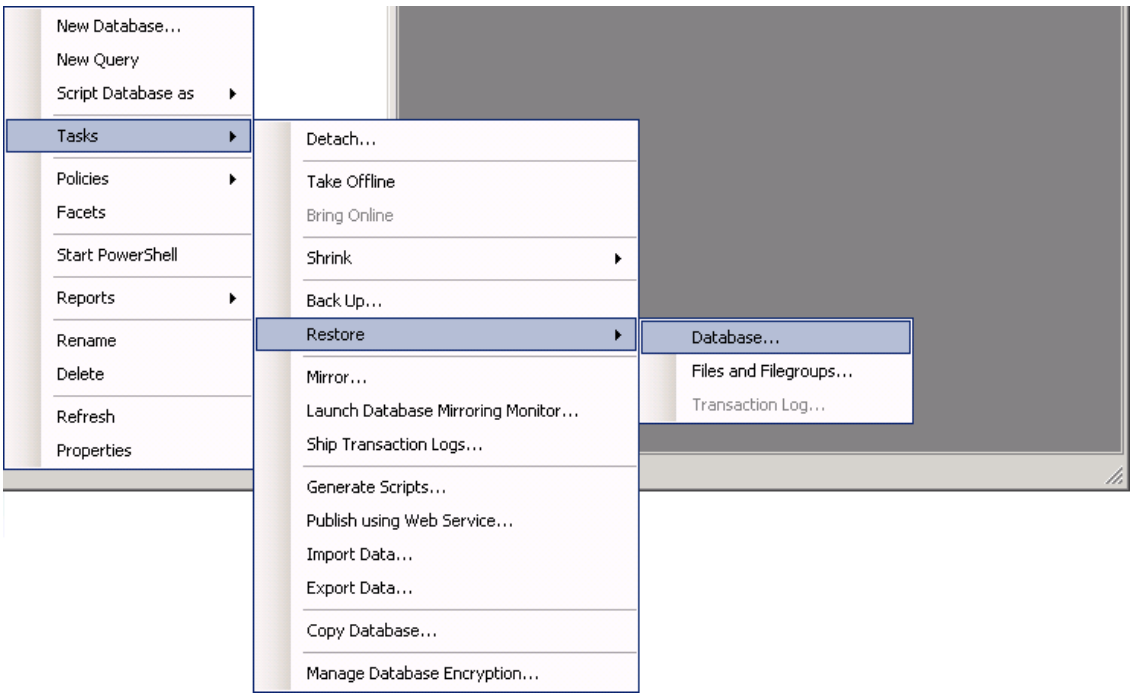
   Depending on the database, either selects a user database or expands [System Databases], and then selects a system database.



3. Right click the database, point to [Tasks], clicks [Restore], and then click [Database].

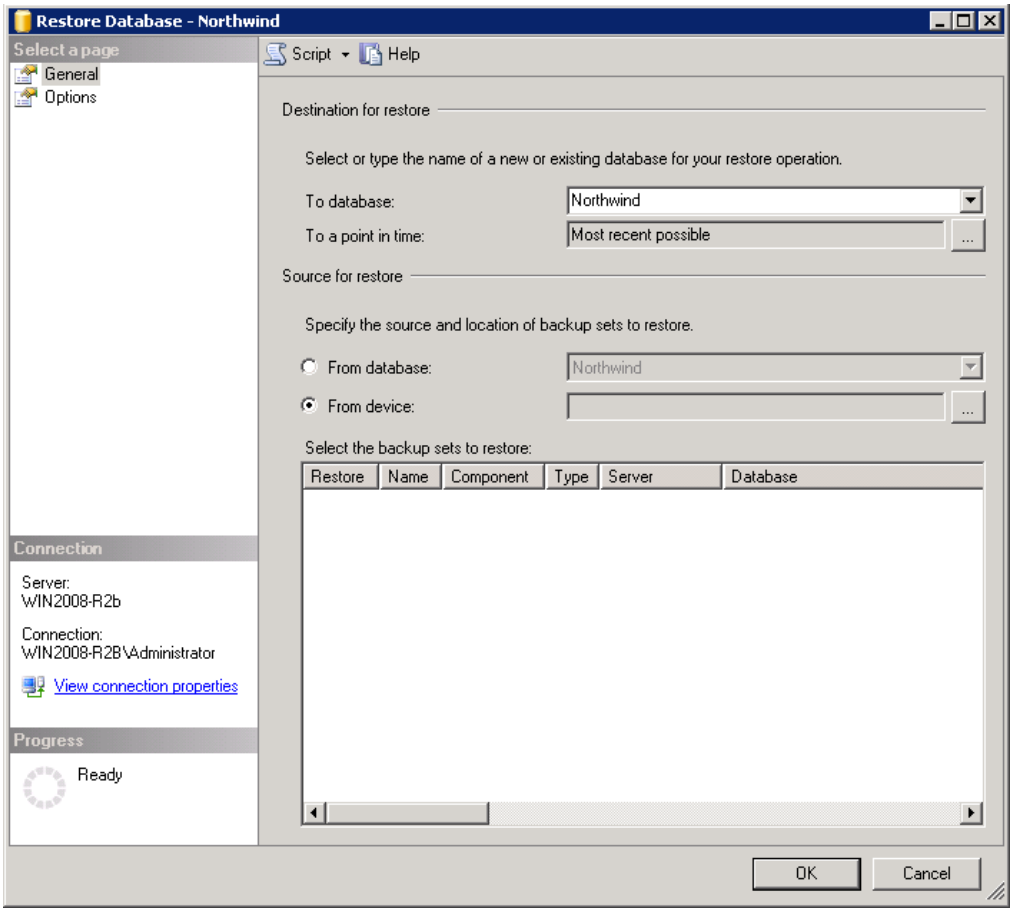
Note:
SQL Server databases may be backed up on one server and restored to another server.

If the target database does not exist on the server, right click on any database instead. A new database can be created while restoring the backup.



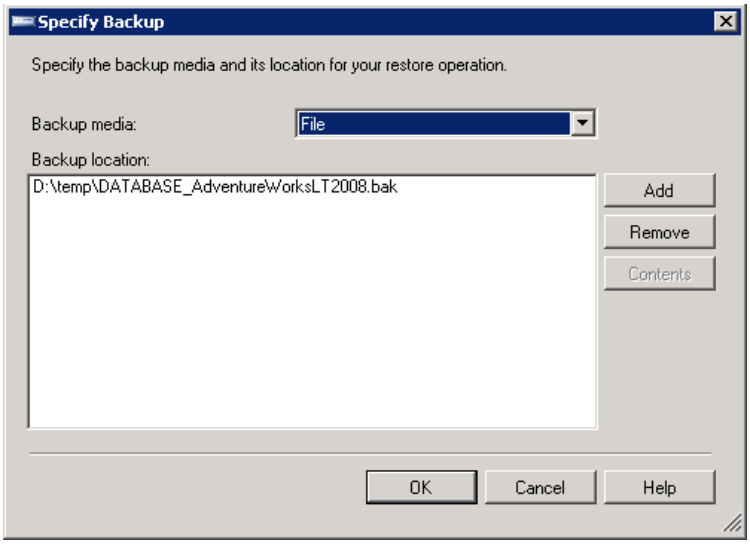
4. On the General page, the name of the restoring database appears in the [To database] list box.

   To create a new database, enter its name in the list box.



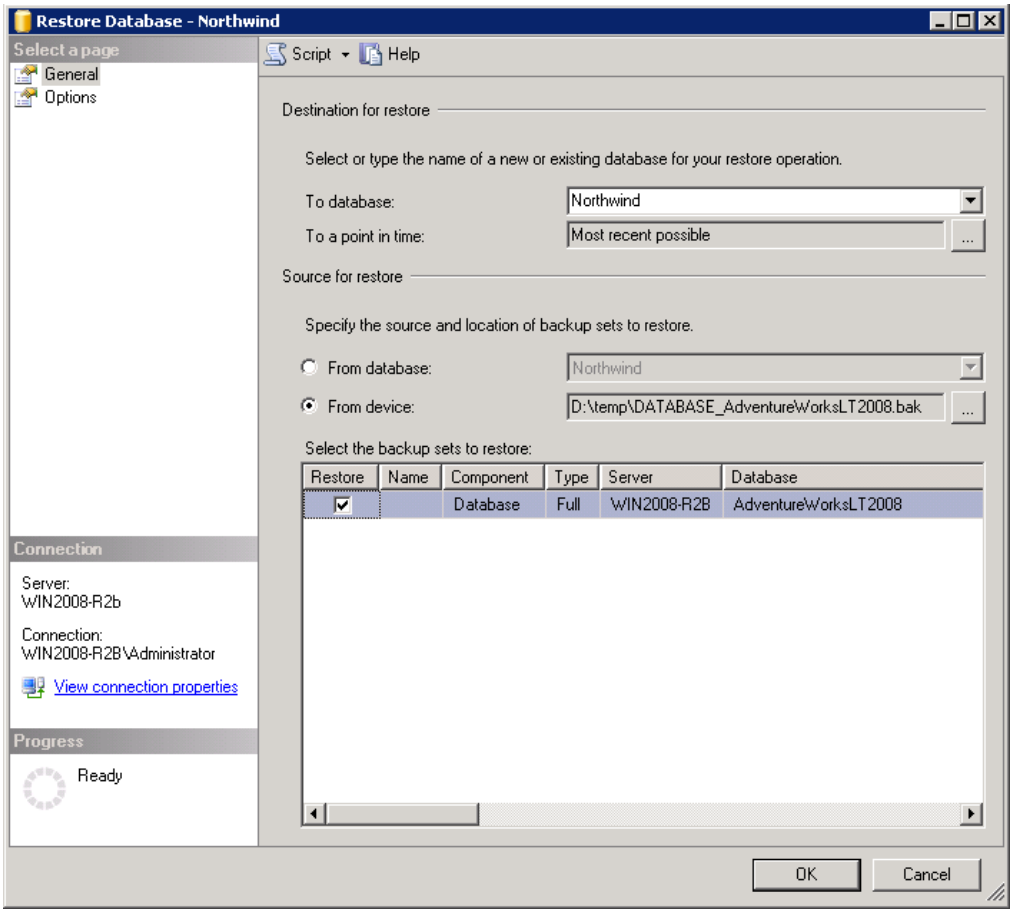
5. Select [From device]; click the browse button to open the [Specify Backup] dialog box. Click [Add].

6. Browse to the backup file (restored from OBS) that is to be restored.



7. After adding the complete database file to the [Backup location] list box, click [OK] to return to the General page.

8. In the [Select the backup sets to restore] grid, select the backups to restore.

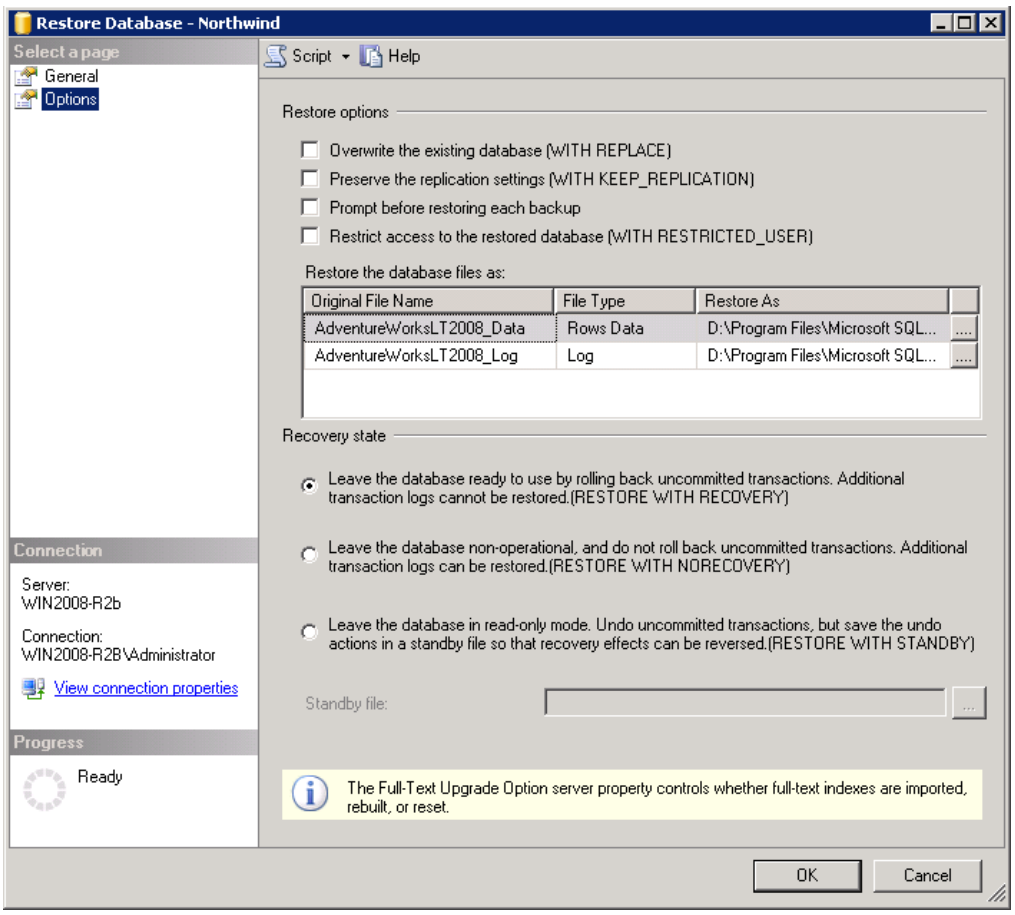


9. Click the Options page and select appropriate options for the restore operation.

   For the [Recovery state] setting:

   Important:
   If this is the final backup to be restored, select -
   [Leave database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored]

   If there are further differential or transaction log to be applied, selection one of the other two options for the Recovery completion state.


Restore Database - Northwind
Select a page
General
Options
Script
Help
Restore options
Overwrite the existing database (WITH REPLACE)
Preserve the replication settings (WITH KEEP_REPLICATION)
Prompt before restoring each backup
Restrict access to the restored database (WITH RESTRICTED_USER)
Restore the database files as:
Original File Name
File Type
Restore As
AdventureWorksLT2008_Data
Rows Data
D:\Program Files\Microsoft SQL...
AdventureWorksLT2008_Log
Log
D:\Program Files\Microsoft SQL...
Recovery state
Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored.(RESTORE WITH RECOVERY)
Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be restored.(RESTORE WITH NORECOVERY)
Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a standby file so that recovery effects can be reversed.(RESTORE WITH STANDBY)
Standby file:
Connection
Server:
WIN2008-R2b
Connection:
WIN2008-R2B\Administrator
View connection properties
Progress
Ready
The Full-Text Upgrade Option server property controls whether full-text indexes are imported, rebuilt, or reset.
OK
Cancel

10. To start the restore operation, click OK.

11. Continue to the next section to restore differential or transaction log backup.

18.5.3.2 Restore other system or user database (differential / transaction log backup)

Refer to the following instructions to restore a differential or transaction log backup:

1. Open SQL Server Management Studio; connect to the server where the backup is to be restored.

   Important:
   Backups must be restored in the order in which they were created.

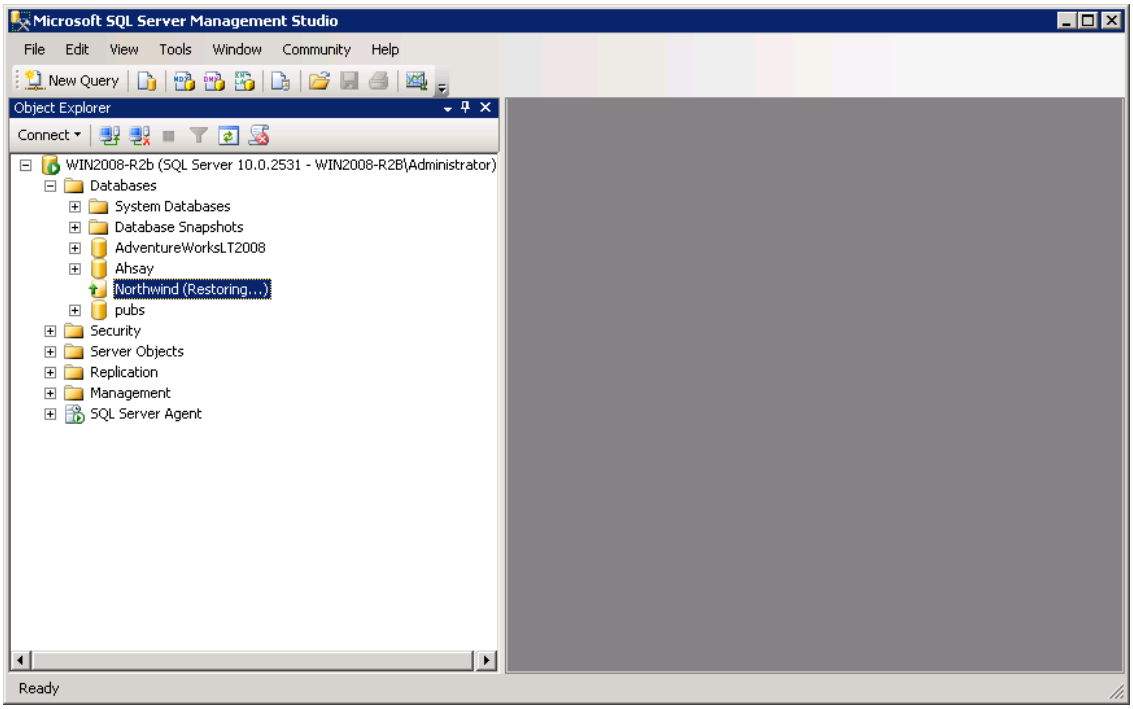
   Transaction log can only be applied to database in *WITH NORECOVERY* recovery state.

   If the database to be restored is not in *NORECOVERY* recovery state, restore the previous backup using the following recovery state option:

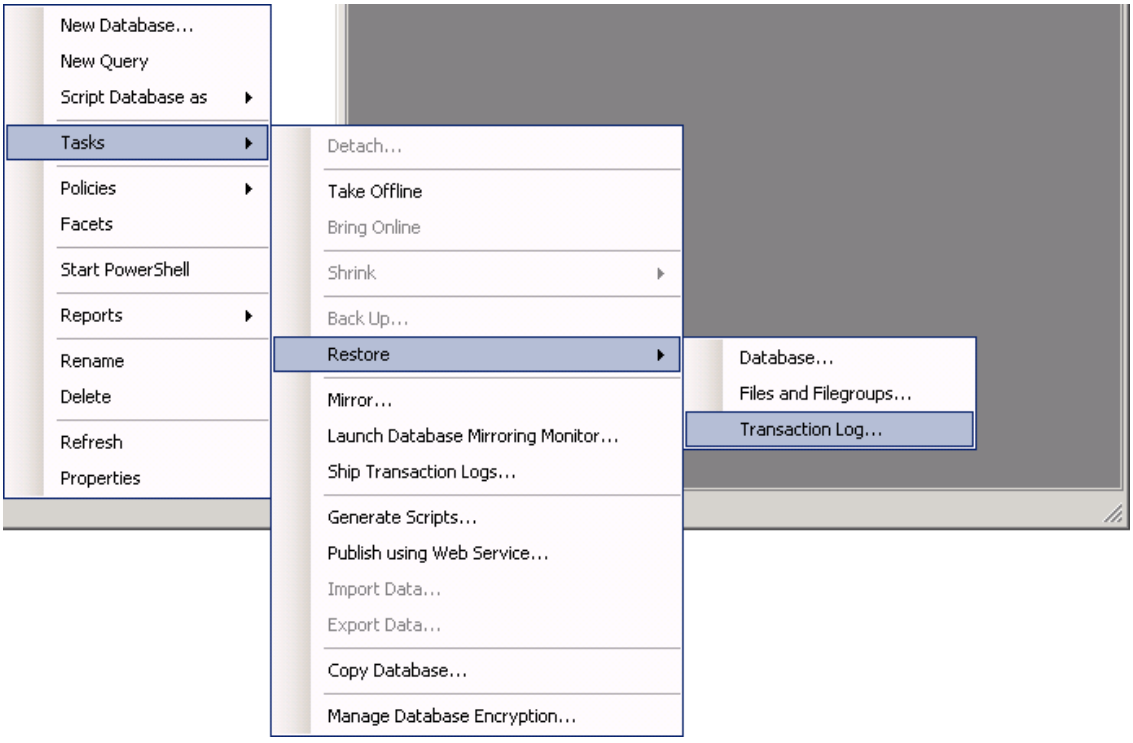
[Leave the database non-operational, and do not roll back the uncommitted transactions. Additional transaction logs can be restored].

2. Expand [Databases].

   Select the corresponding user database or system database.

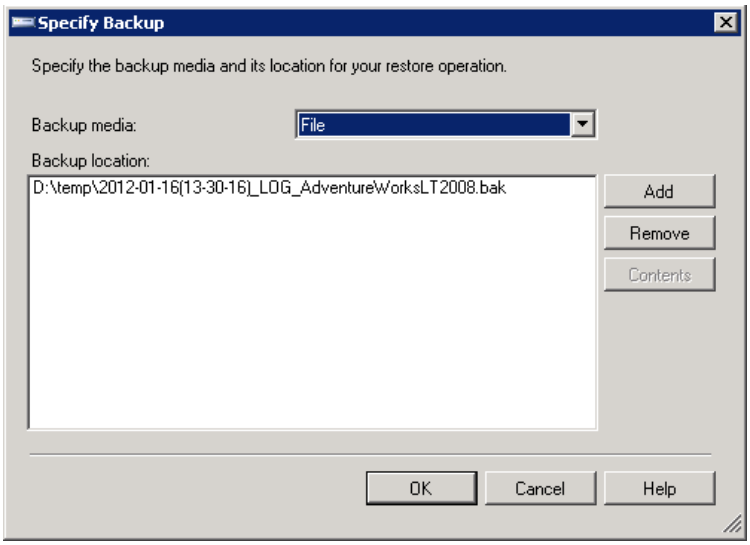


3. Right click the database, [Tasks], [Restore], and then click [Database] or [Transaction Log] according to the backup file you are restoring.



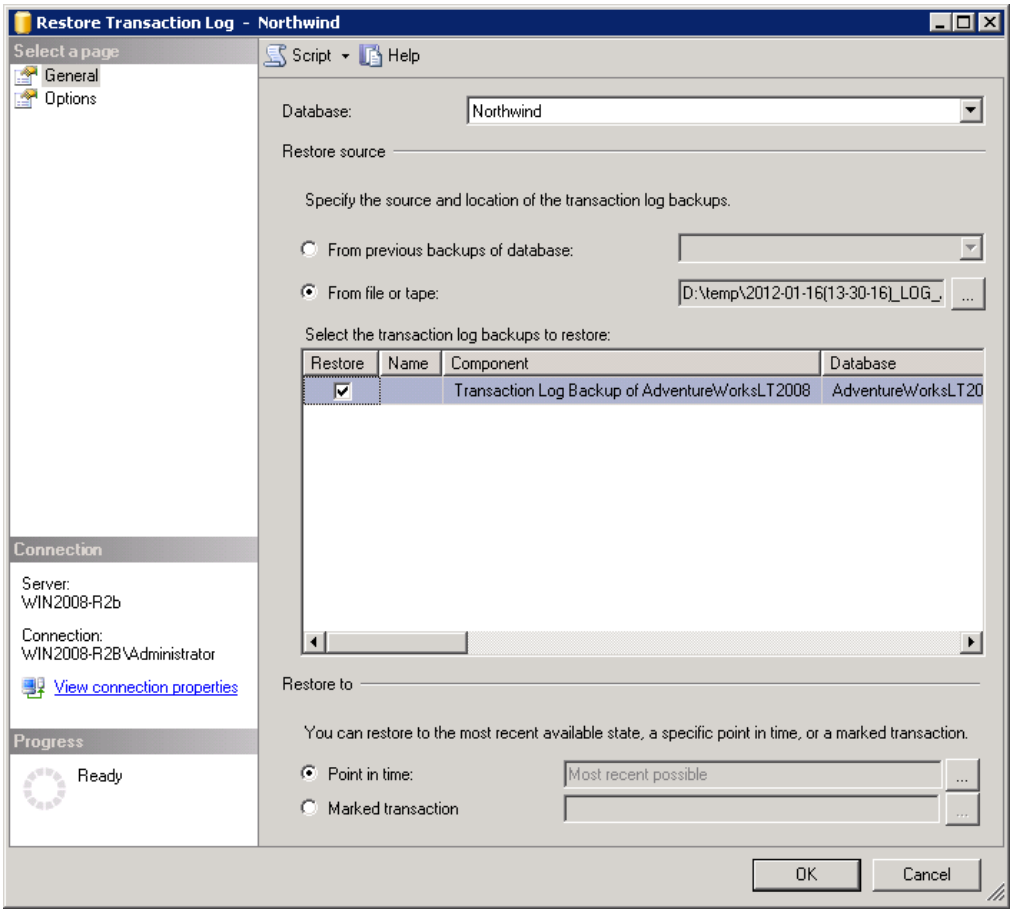
4. Select [From file or tape]; click the browse button to open the [Specify Backup] dialog box. Click [Add].

5. Browse to the backup file (restored from OBS) that is to be restored.



6. After adding the differential database or transaction log file to the [Backup location] list box, click [OK] to return to the General page.

7. In the [Select the backup sets to restore] grid, select the backups to restore.

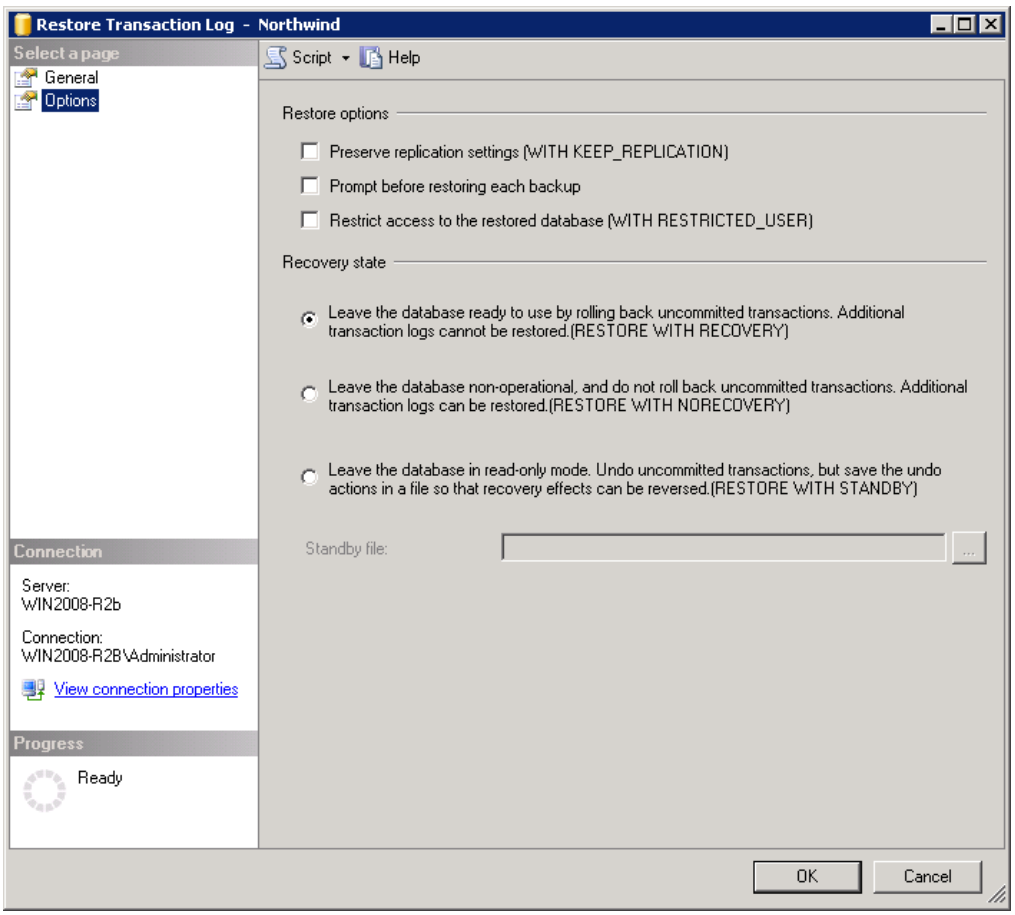


8. Click the Options page and select appropriate options for the restore operation.

   For the [Recovery state] setting:

   Important:
   If this is the final backup to be restored, select [Leave database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored].

   If there are further differential or transaction log to be applied, selection one of the other two options for the Recovery completion state.


Restore Transaction Log - Northwind
Select a page
General
Options
Script
Help
Restore options
Preserve replication settings (WITH KEEP_REPLICATION)
Prompt before restoring each backup
Restrict access to the restored database (WITH RESTRICTED_USER)
Recovery state
Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored.(RESTORE WITH RECOVERY)
Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be restored.(RESTORE WITH NORECOVERY)
Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a file so that recovery effects can be reversed.(RESTORE WITH STANDBY)
Standby file:
Connection
Server:
WIN2008-R2b
Connection:
WIN2008-R2B\Administrator
View connection properties
Progress
Ready
OK
Cancel

9. To start the restore operation, click OK.

19 Backup / Restore Lotus Domino and Notes

This chapter describes how to backup and restore Lotus Domino Server and Notes Client with OBM.

19.1 Supported versions

The Lotus Domino Server and Lotus Notes Client backup modules are supported for the following Lotus Domino / Notes versions:

- Lotus Domino / Notes 8.5.0
- Lotus Domino / Notes 8.5.1

Note:
Lotus Domino / Notes 8.5.2 are **not** supported.

For more details, please refer to Help Centre Article:
https://help..com/openArticle.aspx?aid=2323

19.2 Limitation

Backup of **Lotus Notes is only** supported for installation on **Windows**.

19.3 Requirements and recommendations

Please ensure that the following requirements are met by the Lotus Domino server or Lotus Notes client computer:

1. OBM is installed on the Lotus Domino server or Lotus Notes client machine.

2. Data selected for backup will be temporarily spooled to a temp directory before being uploaded to the backup server.

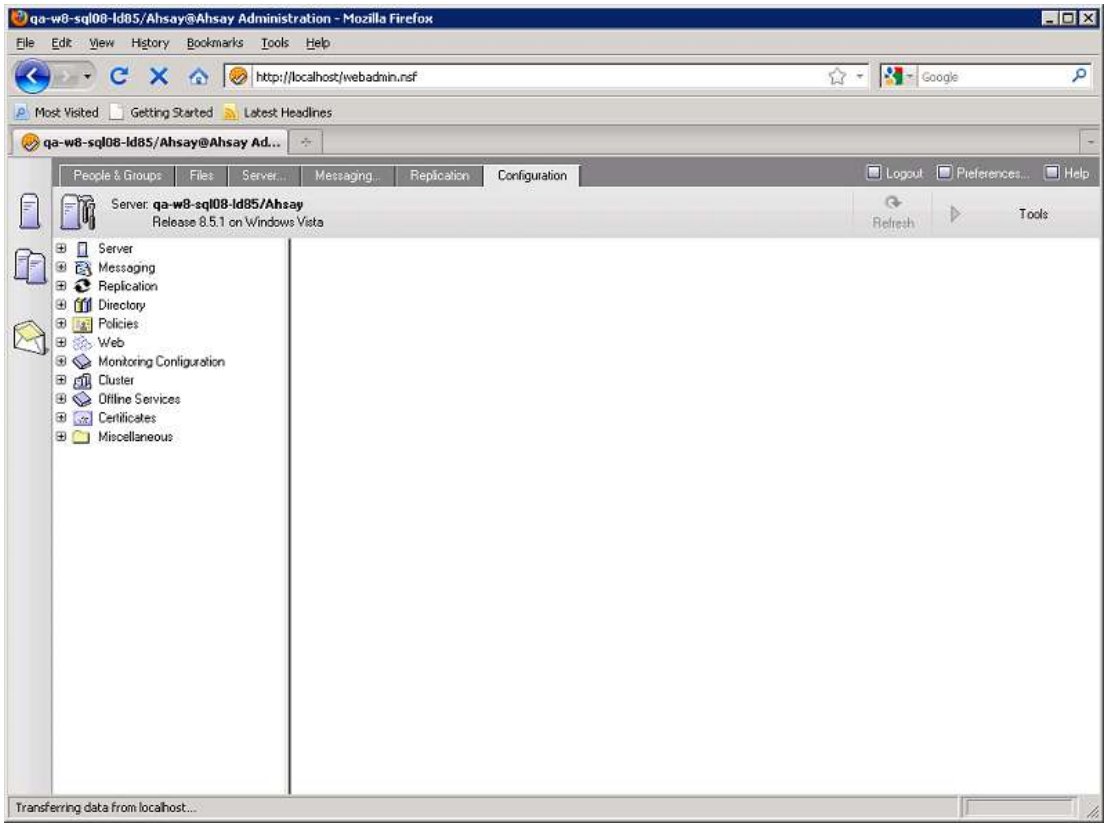
   Please ensure that the temporary directory configured for the backup have sufficient disk space for the backup operation.

3. For backup of Lotus Domino server, all database selected for backup must have transaction logging (archive mode) enabled.

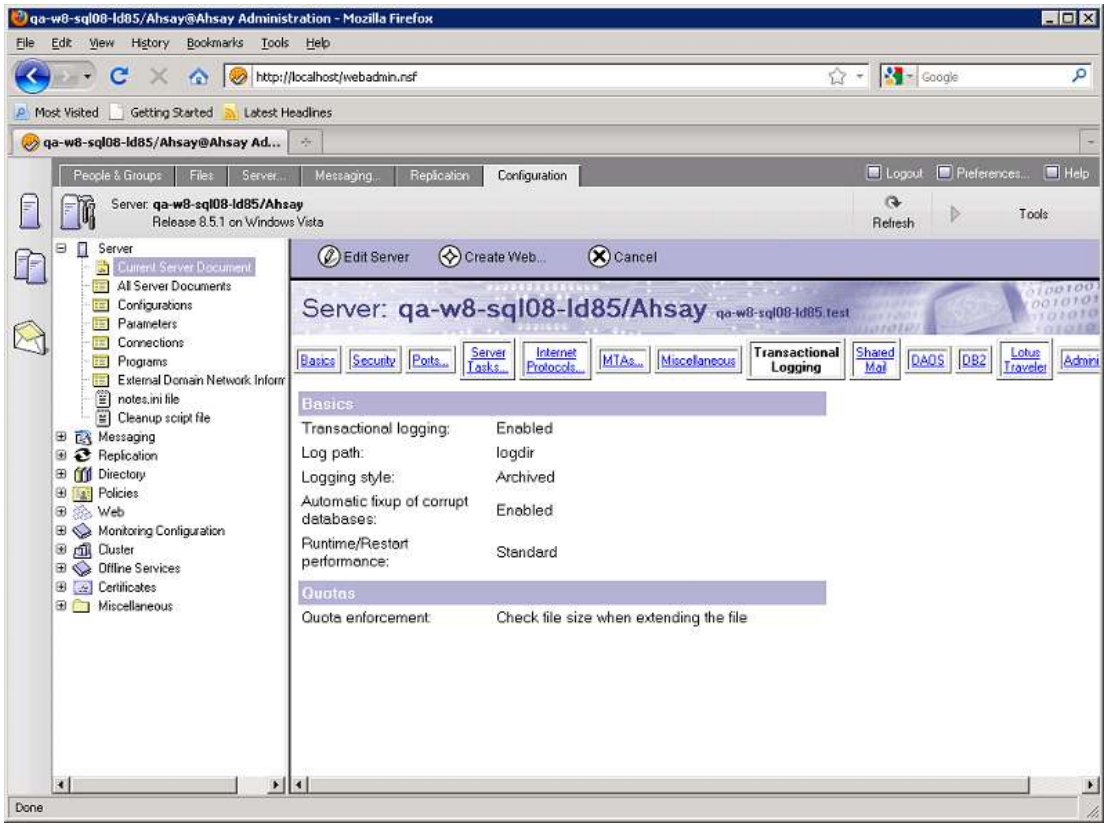
   Note:
   Ensure that all databases to be logged reside in the Domino data directory, either at the root or in sub directories

   To configure transaction logging, please refer to the following instruction:

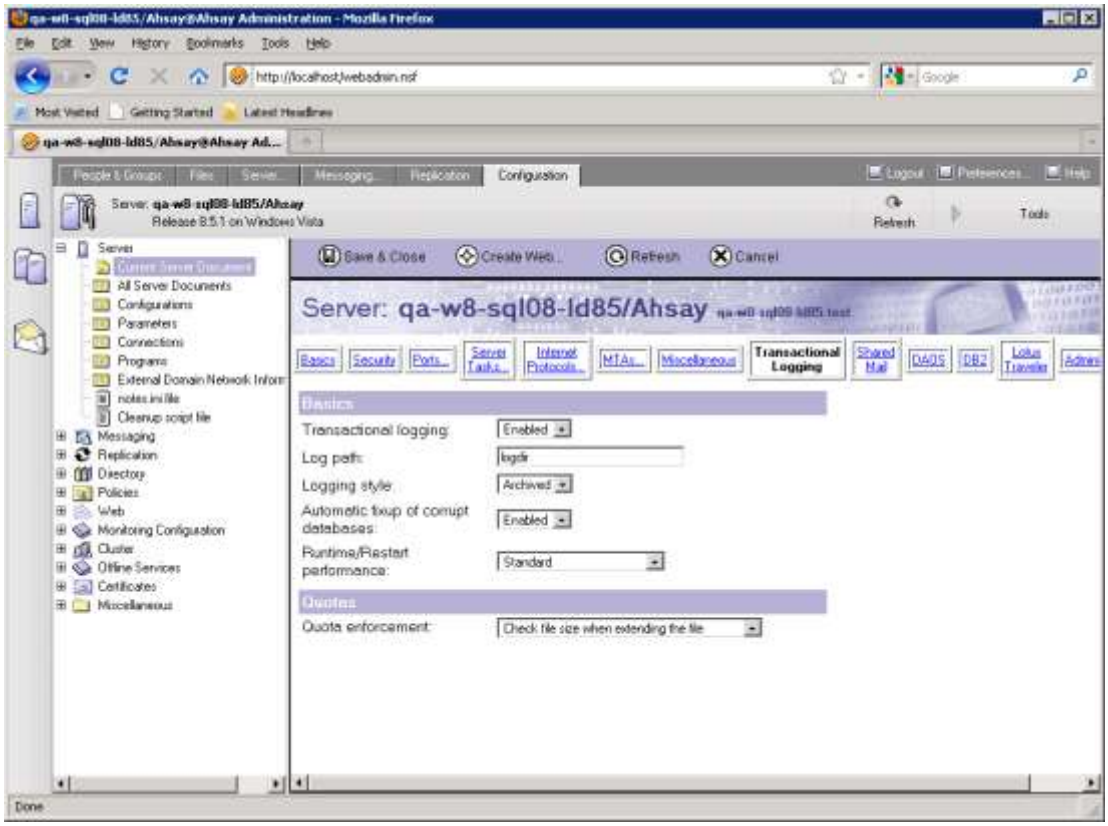
   - Login to the Domino administration console; select the [Configuration] tab.



- Expand [Server], then [Current Server Document].



- Select the [Transaction Logging] tab, then [Edit Server].



- Complete all required fields then save the document afterward.

Field	Enter
Transaction Logging	**Choose Enabled. The default is Disabled.**
Log Path	**Path name location of the transaction log.** **There should be at least 1GB of disk space for the transaction log.** **If you are using the device solely for storing the transaction log, set the [Use all available space on log device] field to "Yes"**
Logging Style	**Choose [Archive]. The default is [Circular].**
Maximum Log Space	**The maximum size in MB, for the transaction log. Default is 192MB. Maximum is 4096MB (4GB).**

	Domino formats at least 3 and up to 64 log files, depending on the maximum log space you allocate.
Use all available space on log device	**Choose one:** **[Yes] -** **To use all available space on the device for the transaction log. This is recommended if you use a separate device dedicated for storing the log. If you choose [Yes], you do not need to enter a value in the [Maximum Log Space] field.** **[No] -** **To use the default or specified value in the [Maximum Log Space] field.**
Automatic fixup of corrupt databases	**Choose one:** **Enabled (default) -** **If a database is corrupted and Domain cannot use the transaction log to recover it, Domino runs the Fixup task, assigned a new DBIID, and notifies the administrator that a new database backup is required.** **Disabled -** **Domino does not run the Fixup task automatically and notifies the administrator to run the Fixup task with the -J parameter on corrupt logged databases.**
Runtime / Restart performance	**This field controls how often Domino records a recovery checkpoint in the transaction log, which affects server performance.** **To record a recovery checkpoint, Domino evaluates each active logged database to determine how many transactions would be necessary to recover each database after a system failure. When Domino completes this evaluation, it:** **1. Creates a recovery checkpoint record in the transaction log, listing each open database and the starting point transaction needed for recovery.**

	2. Force database changes to be saved to disk if they have not been saved already **Choose one:** **Standard (default and recommended) - Checkpoints occur regularly.** **Favor runtime -** **Domino records fewer checkpoints, which requires fewer system resources and improves server run time performance.** **Favor restart -** **Recovery time. Domino records more checkpoints, which improves restart recovery time because fewer transactions are required for recovery.**

Note:
Transaction log backup can only be performed if the transaction logging option is enabled in archive mode.

19.4 Overview

The following steps are performed during a backup job:

1. Connection from the backup client to the backup server is established.

2. Download the server file list from the backup server.

3. For [Database] backup type, the following data are backed up to the temporary spool path:

   - notes.ini
   - All file selected
   - All database selected
   - Transaction log

   The Domino server is notified of the filled log extends availability for reuse.

4. *Lotus Domino Server only* - For [Transaction Log] backup type, only transaction logs are backed up to the temporary spool path.

   The Domino server is notified of the filled log extends availability for reuse

5. Server and local file lists are compared to determine which file will be uploaded.

6. Delta file is generated for modified file (if necessary).

7. Data are encrypted, compressed, and uploaded to the backup server.

8. Data are removed from the temporary spool path.

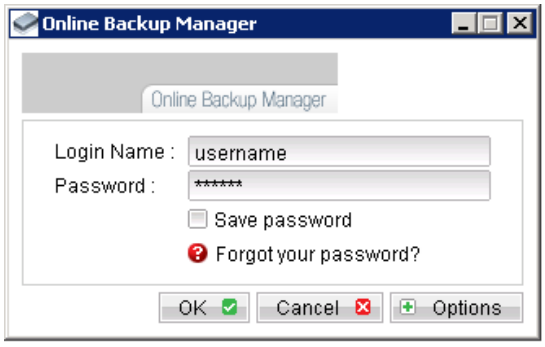
9. Backup completed successfully.

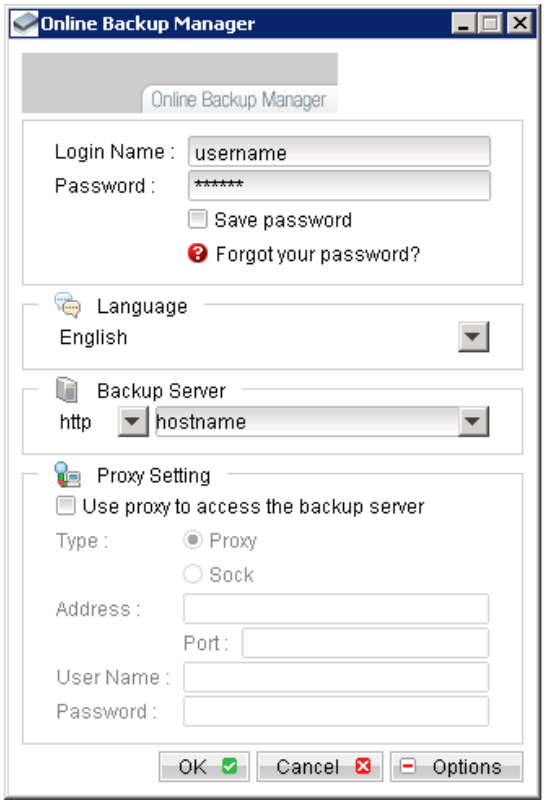
19.5 How to backup Lotus Domino / Notes (Windows)

Refer to the following instructions to backup Lotus Domino / Notes installation on Windows:

1. Login to the backup application's user interface.

   Double-click on the OBM desktop icon or right-click on the system tray icon:

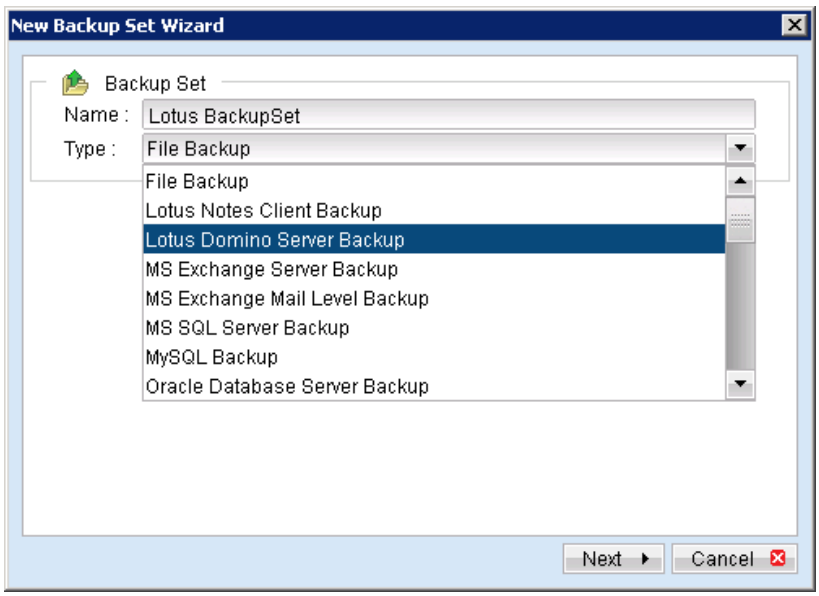




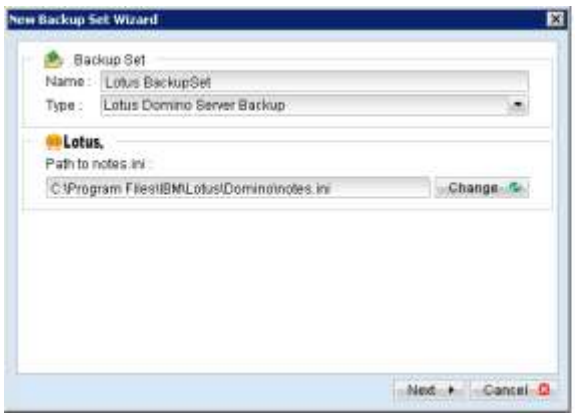
   Note:
   OBM must be installed on the Lotus Domino server or Notes client machine.

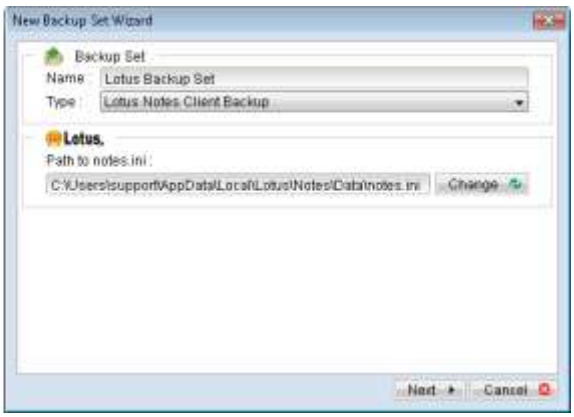
2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

3. Create a Lotus Domino Server or Notes Client Backup set by selecting [Lotus Domino Server Backup] / [Lotus Notes Client Backup] from the backup set type dropdown menu.



4. Configure the [Path to notes.ini] field, and then select [Next] to proceed.





Note:
[Path to notes.ini] on **Lotus Domino server**:

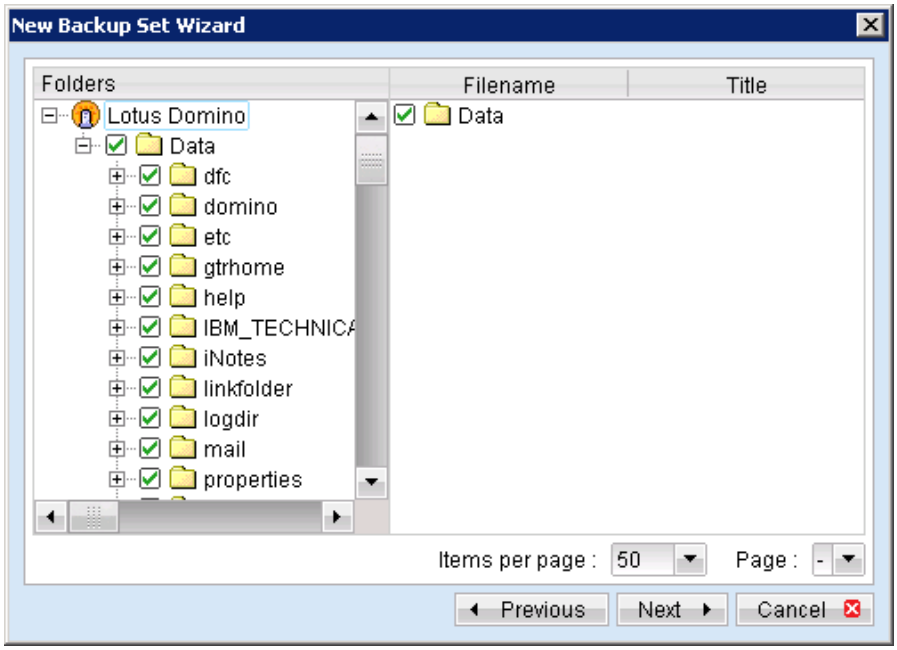
Login to the Domino administration console, select the [Configuration] tab, and expand [Server], select [notes.ini file] to display the directory path.

[Path to notes.ini] on **Lotus Notes client machine**:

By default, the path should be located under the corresponding operating system account profile:

${OS_Profile}\AppData\Local\Lotus\Notes\Data\notes.ini

5. Select the file and database for backup.



6. Configure a backup schedule for unattended backups.

   Note:
   Multiple backup schedules of different types can be configured for the same backup set.

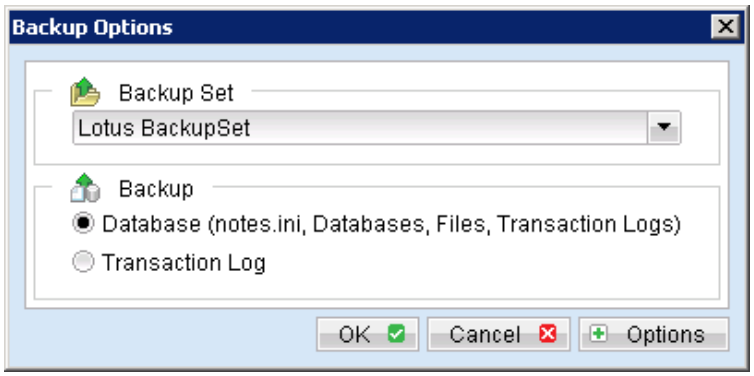
7. Select an encryption setting for your backup set.

8. Press the [OK] button to complete the configuration of backup set.

9. Scheduled backup will run automatically at the configured schedule time.

10. Click [Backup] button on the left panel to perform a backup immediately.

11. Select the backup type to be performed:



Menu Items	Description
Database (notes.ini, Database, Files, Transaction Logs)	Backup the following: notes.ini All file selected All database selected

	Transaction log
Transaction Log	Backup the transaction log.

19.6 How to restore Lotus Domino / Notes (Windows)

Refer to the following instructions to restore Lotus Domino / Notes installation on Windows:

1. Install OBM on the Lotus Domino server or Lotus Notes client machine (if required).

2. Restore the Lotus databases / files from backup; restore the database backup files from the OBS server.

3. Shutdown the Lotus Domino services.

4. Continue to the next section for instruction to restore all databases or single database.

Restore all databases and files
To perform a full Domino restore (restore all databases and files):

5. Place the restored backup files to their original directory path:

   Database files, notes.ini and archived transaction logs are stored on OBS along with their full path information.

   Place the files back to their original location (location where the backup was originally performed).

6. Start the Lotus Domino services.

7. In the OBM installation bin folder, open "DominoRecover.bat" with a text editor.

   Modify the *User Defined Section* according to your setup:

User Defined Parameters	Description
PROGRAM_DIR (For all / single db restore)	Directory containing the notes.ini file.
INPUT_FILE (For single db restore)	Path to the input file.
RESTOREDB (For single db restore)	Path to the database file.
RECDATE (For single db restore)	The year, month day to recover database to.
RECTIME (For single db restore)	The time in hour and minute to recover database to.

   Example:

DominoRecover.bat:

```
REM ############  Start: User Defined Section ##############

REM ###################### PROGRAM_DIR ######################
REM ## The Domino or notes program directory, which
REM ## contains notes.ini
SET PROGRAM_DIR=C:\Program Files\Lotus\Domino

REM ###################### INPUT_FILE ######################
REM ## The path to a input file if you want to restore one
REM ## database only. If you want to restore all databases,
REM ## leave INPUT_FILE blank.
SET INPUT_FILE=

REM ###################### RESTOREDB ######################
REM ## The path to a database file if you want to restore
REM ## one database only. If you want to restore all
REM ## databases, leave RESTOREDB blank.
SET RESTOREDB=

REM ###################### RECDATE ######################
REM ## The year, month and day you want to recover
REM ## the database to. Set them according to the date
REM ## format set in Windows.
REM ## e.g. SET RECDATE=11/15/2006
REM ## If you want to restore all databases, leave RECDATE
REM ## blank.
REM ## e.g. SET RECDATE=
SET RECDATE=

REM ###################### RECTIME ######################
REM ## The time in hour and minute you want to recover the
REM ## database to. Set them according to the time format
REM ## set in Windows.
REM ## e.g. SET RECTIME=13:00
REM ## If you want to restore all databases, leave RECTIME
REM ## blank.
REM ## e.g. SET RECTIME=
SET RECTIME=
```

8. Save, and execute the "DominoRecover.bat" batch file afterward:

```
>C:\Program Files\OBM\bin\DominoRecover.bat
```

Media recovery is performed for all databases found within the Lotus data directory.

Content of all databases will be restored to the last committed transaction found in the archived transaction log.

Example:

```
C:\Program Files\OBM\bin>DominoRecover.bat
Media Recovery Utility for Lotus Domino 5.0 or above

Please make sure that you have done the following:
1. Reinstall Lotus Domino on this computer in the same
directory
2. Restore Notes.ini to the Lotus Domino installation
directory
   (e.g. C:\Lotus\Domino)
3. Restore Domino Data directory back to the directory
defined
   in Notes.ini (e.g. C:\Lotus\Domino\Data)
4. Restore all archived transaction logs to the directory
defined
   in Notes.ini (e.g. C:\Lotus\Domino\Data\logdir)

Continue? (Y) or (N) y
Running media recovery ...
Please wait, creating new transaction logs in directory:
C:\logdir\
02/12/2003 14:39:19   Recovery Manager: Restart Recovery
complete. (0/0
databases needed full/partial recovery)
Media Recovery Replay (122 MB): 10% 20% 30% 40% 50% 60% 70%
80% 90% 100%
02/12/2003 14:39:22   Recovery Manager: Media Recovery
complete for
C:\Lotus\Domino\Data\admin4.nsf, last update applied.

 Backup file C:\Lotus\Domino\Data\admin4.nsf recovered.

.....

Media Recovery Replay (122 MB): 10% 20% 30% 40% 50% 60% 70%
80% 90% 100%
02/12/2003 14:40:57   Recovery Manager: Media Recovery
complete for
C:\Lotus\Domino\Data\statrep.nsf, last update applied.

 Backup file C:\Lotus\Domino\Data\statrep.nsf recovered.

C:\program files\obm\bin>
```

9. Restart the Lotus Domino services.

Restore a single database
To restore a single database:

5. Place the restored database file to the original directory path:

   Database and archived transaction logs are stored on OBS along with their full path information, place them back to their original location (location where the backup was originally performed).

6. *Optional for media recovery* - Place the restored archived transaction logs to their original directory path.

7. In the OBM installation bin folder, open "DominoRecover.bat" with a text editor.

   Modify the *User Defined Section* according to your setup:

User Defined Parameters	Description
PROGRAM_DIR (For all / single db restore)	Directory containing the notes.ini file.
INPUT_FILE (For single db restore)	Path to the input file.
RESTOREDB (For single db restore)	Path to the database file.
RECDATE (For single db restore)	The year, month day to recover database to.
RECTIME (For single db restore)	The time in hour and minute to recover database to.

   To restore a database named "admin4.nsf", and have been placed to "C:\restore_dest", you need to amend the following parameters:

DominoRecover.bat:

```
REM ############  Start: User Defined Section ##############

REM ###################### PROGRAM_DIR ######################
REM ## The Domino or notes program directory, which
REM ## contains notes.ini
SET PROGRAM_DIR=C:\Program Files\Lotus\Domino

REM ###################### INPUT_FILE ######################
REM ## The path to a input file if you want to restore one
REM ## database only. If you want to restore all databases,
REM ## leave INPUT_FILE blank.
SET INPUT_FILE=C:\restore_dest\admin4.nsf

REM ###################### RESTOREDB ######################
```

```
REM ## The path to a database file if you want to restore
REM ## one database only. If you want to restore all
REM ## databases, leave RESTOREDB blank.
SET RESTOREDB=C:\Lotus\Domino\Data\admin4.nsf

REM ######################## RECDATE ##########################
REM ## The year, month and day you want to recover
REM ## the database to. Set them according to the date
REM ## format set in Windows.
REM ## e.g. SET RECDATE=11/15/2006
REM ## If you want to restore all databases, leave RECDATE
REM ## blank.
REM ## e.g. SET RECDATE=
SET RECDATE=18/01/2007

REM ######################## RECTIME ##########################
REM ## The time in hour and minute you want to recover the
REM ## database to. Set them according to the time format
REM ## set in Windows.
REM ## e.g. SET RECTIME=13:00
REM ## If you want to restore all databases, leave RECTIME
REM ## blank.
REM ## e.g. SET RECTIME=
SET RECTIME=00:02
```

8. Save, and execute the "DominoRecover.bat" batch file afterward.

```
>C:\Program Files\obm\bin\DominoRecover.bat
```

Media recovery is performed for the specified database.

Content of the database will be restored to the last committed transaction found in the archived transaction log.

Example:

```
C:\Program Files\OBM\bin>DominoRecover.bat
Media Recovery Utility for Lotus Domino 5.0 or above

Running media recovery ...
Restart Analysis (0 MB): 100%
18/01/2007 14:42:15   Recovery Manager: Restart Recovery
complete. (0/0
databases needed full/partial recovery)
Media Recovery Replay (122 MB): 10% 20% 30% 40% 50% 60% 70%
80% 90% 100%
18/01/2007 14:42:17   Recovery Manager: Media Recovery
complete for
C:\Lotus\Domino\data\admin4.nsf, last update applied.

 Backup file C:\Lotus\Domino\data\admin4.nsf recovered.
```

```
C:\Program Files\OBM\bin>DominoRecover.bat
```

9. Restart the Lotus Domino services.

19.7 How to backup Lotus Domino (Linux)

Refer to the following instructions to backup Lotus Domino installation on Linux:

1. Install OBM on the Lotus Domino server.

   Note:
   OBM must be installed on the Lotus Domino server

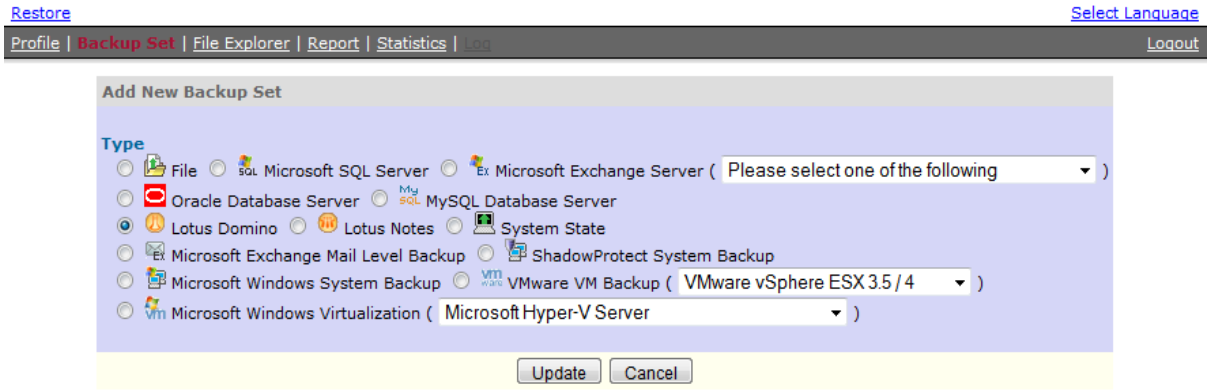
   Important:
   Please ensure that the operating system account to run OBM has sufficient permission to access the following file:

   $OBM_HOME/bin/notesenv

2. Create a new Lotus Domino backup set on the web interface.

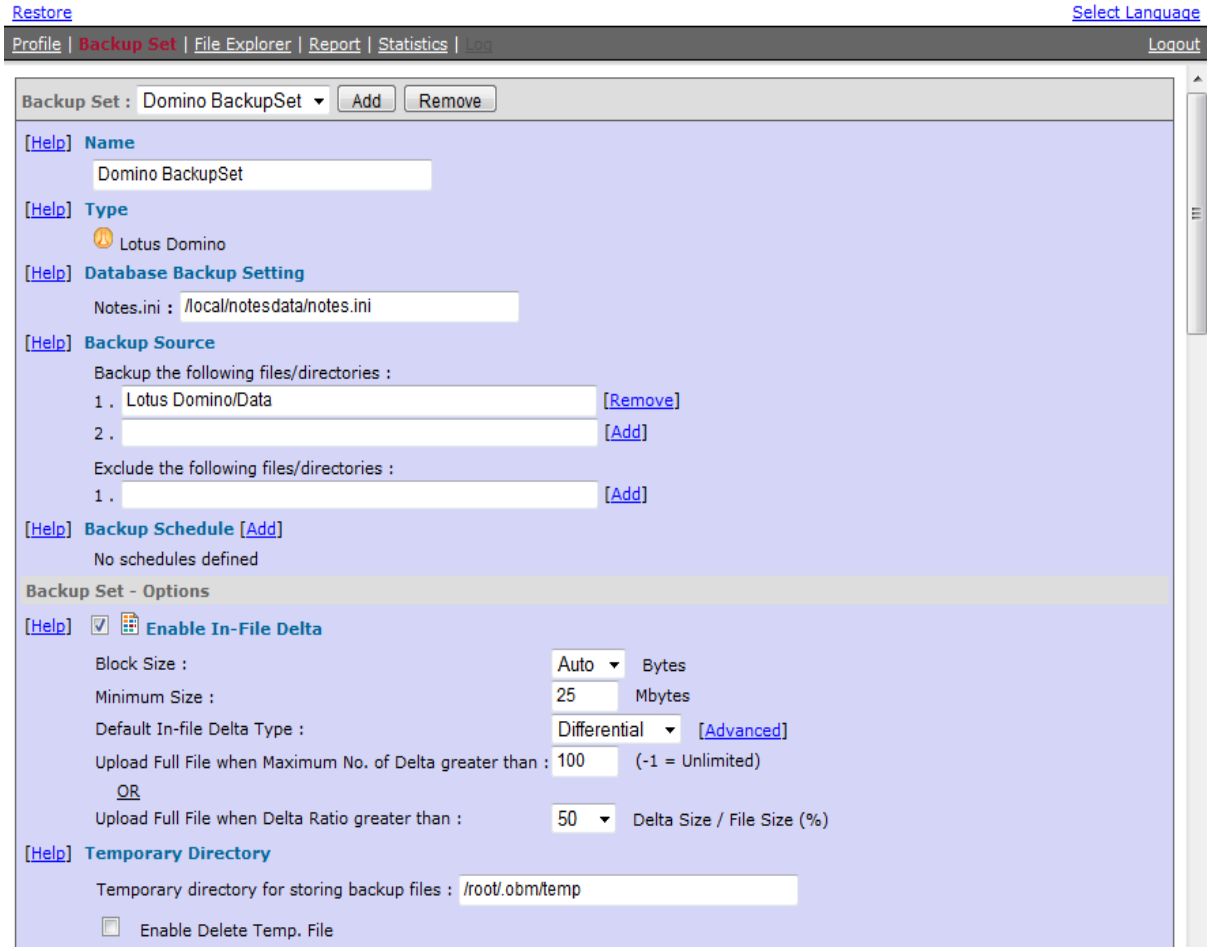
3. Login to the OBS web console, select [Backup Set].

4. Press the [Add] button to access the Add New Backup Set menu.



5. Select the [Lotus Domino] radio button and [Update].

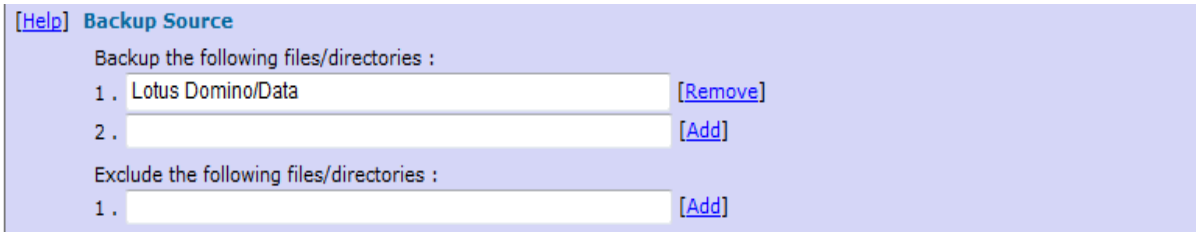
6. Enter the Name and Backup Setting required:


Restore
Select Language
Profile | Backup Set | File Explorer | Report | Statistics | Log
Logout
Backup Set : Domino BackupSet
Add
Remove
[Help] Name
Domino BackupSet
[Help] Type
Lotus Domino
[Help] Database Backup Setting
Notes.ini : /local/notesdata/notes.ini
[Help] Backup Source
Backup the following files/directories :
1 . Lotus Domino/Data
[Remove]
2 .
[Add]
Exclude the following files/directories :
1 .
[Add]
[Help] Backup Schedule [Add]
No schedules defined
Backup Set - Options
[Help] Enable In-File Delta
Block Size : Auto Bytes
Minimum Size : 25 Mbytes
Default In-file Delta Type : Differential [Advanced]
Upload Full File when Maximum No. of Delta greater than : 100 (-1 = Unlimited)
OR
Upload Full File when Delta Ratio greater than : 50 Delta Size / File Size (%)
[Help] Temporary Directory
Temporary directory for storing backup files : /root/.obm/temp
Enable Delete Temp. File

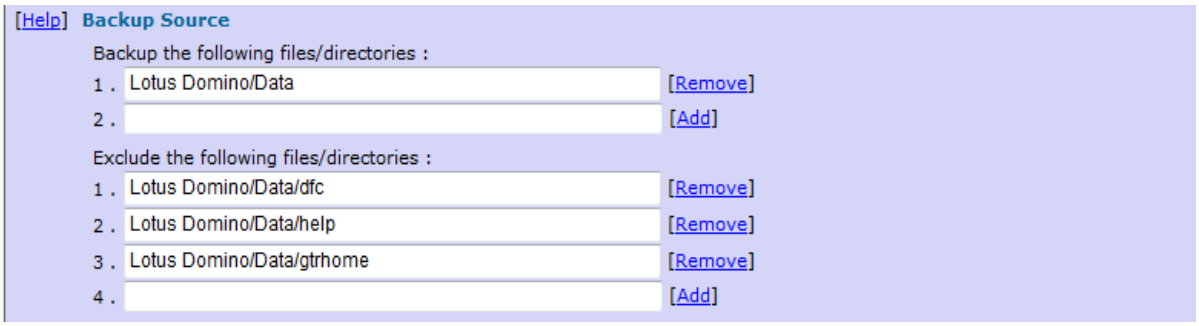
Menu Items	Description
Name	Enter a backup set name of your choice.
Database Backup Setting	Enter the directory path to the notes.ini file. Default location is: /local/notesdata/notes.ini
Temporary Directory	Enter the directory path of the temporary spool path. Please ensure that the user running OBM has sufficient permission to access this location and sufficient space is available.

7. Enter the Backup Source required:

   To backup all data, enter "Lotus Domino/Data" in the [Backup the following files/directories] field:



To backup or exclude individual data, enter the corresponding directory path (e.g. Lotus Domino/Data/help):



8. Configure a backup schedule for unattended backups.

   Note:
   Multiple backup schedules of different types can be configured for the same backup set.

9. Press the [Update] button to save the newly created backup set.

10. Login to the Lotus Domino server with OBM installed.

11. Start the Configurator.sh script by accessing the backup client installation bin folder.

```
>sh OBM_HOME/bin/Configurator.sh
```

12. Follow the instructions provided in the Configurator to complete the configuration of the backup set.

    Note:
    For Linux with GUI installed, you can also create a backup set via the OBM user interface (similar to the procedures provided in the Windows section).

    Launch the OBM user interface:

```
>sh OBM_HOME/bin/RunOBC.sh
```

13. Scheduled backup will run automatically at the configured schedule time.

14. To perform a backup immediately, execute the RunBackupSet.sh script with the backup set name or ID:

```
>sh OBM_HOME/bin/RunBackupSet.sh BackupSet_Name
```

Important:
Before executing the script, please edit the BACKUP_TYPE parameter within the RunBackupSet.sh script file from -

BACKUP_TYPE="FILE"

to

BACKUP_TYPE="DATABASE"

19.8 How to restore Lotus Domino / Notes (Linux)

Refer to the following instructions to restore Lotus Domino installation on Linux.

1. Install OBM on the Lotus Domino server (if required).

2. Restore the Lotus databases / files from backup; restore the database backup files from the OBS server.

3. Shutdown the Lotus Domino services.

4. Continue to the next section for instruction to restore all databases or single database.

Restore all databases and files
To perform a full Domino restore (restore all databases and files):

5. Place the restored backup files to their original directory path:

   Database files, notes.ini and archived transaction logs are stored on OBS along with their full path information, place them back to their original location (location where the backup was originally performed).

6. Ensure that the Lotus Domino user is the owner of all restored data, and has write permission to the files.

   To assign such permission:

```
>chown -R notes:notes /local/notesdata
```

7. Start the Lotus Domino services

8. In the OBM installation bin folder, open "DominoRecover.sh" with a text editor.

   Modify the *User Defined Section* according to your setup:

User Defined Parameters	Description
DATA_DIR (For all / single db restore)	Directory containing the notes.ini file.
LOTUS (For all / single db restore)	Directory which the Domino server is installed.
INPUT_FILE (For single db restore)	Path to the input file.
RESTOREDB (For single db restore)	Path to the database file.

RECDATE (For single db restore)	The year, month day to recover database to.
RECTIME (For single db restore)	The time in hour and minute to recover database to.

Example:

DominoRecover.sh:

```
###############  Start: User Defined Section  ##############

# ----------------------- DATA_DIR -----------------------
# | The Domino directory which contains notes.ini,        |
# | the Domino databases, and templates.                  |
# | e.g. DATA_DIR=/local/notesdata                        |
# -------------------------------------------------------
DATA_DIR=/local/notesdata

# ------------------------ LOTUS ------------------------
# | The directory in which all Lotus products for         |
# | UNIX are installed.                                   |
# | e.g. LOTUS=/opt/ibm/lotus                             |
# -------------------------------------------------------
LOTUS=/opt/ibm/lotus

# ---------------------- INPUT_FILE ----------------------
# | The path to an input file if you want to restore      |
# | one database only. If you want to restore all         |
# | databases, leave INPUT_FILE blank.                    |
# -------------------------------------------------------
SET INPUT_FILE=

# ---------------------- RESTOREDB ----------------------
# | The path to a database file if you want to            |
# | restore one database only. If you want to restore     |
# | all databases, leave RESTOREDB blank.                 |
# -------------------------------------------------------
SET RESTOREDB=

# ----------------------- RECDATE -----------------------
# | The year, month and day you want to recover           |
# | the database to. Set them according to the date       |
# | format set in your system.                            |
# | e.g. SET RECDATE=11/15/2006                           |
# | If you want to restore all databases, leave           |
# | RECDATE blank.                                        |
# | e.g. SET RECDATE=                                     |
# -------------------------------------------------------
SET RECDATE=

# ----------------------- RECTIME -----------------------
```

```
# | The time in hour and minute you want to recover the
# | database to. Set them according to the time format
# | set in your system.
# | e.g. SET RECTIME=13:00
# | If you want to restore all databases, leave RECTIME
# | blank.
# | e.g. SET RECTIME=
# ------------------------------------------------------------
SET RECTIME=
```

9. Save, and execute the "DominoRecover.sh" script file afterward:

```
>usr/local/obm/bin/DominoRecover.sh
```

Important:
Please ensure that you are running as the Domino user (e.g. notes)

Media recovery is performed for all databases found within the Lotus data directory.

Content of all databases will be restored to the last committed transaction found in the archived transaction log.

Example:

```
bash-3.00$ cd /usr/local/obm/bin
bash-3.00$ ./DominoRecover.sh
Media Recovery Utility for Lotus Domino 5.0 or above

Please make sure that you have done the following:
1. Reinstall Lotus Domino on this computer in the same
directory
2. Restore Notes.ini to the Lotus Domino installation
directory
   (e.g. /local/notesdata)
3. Restore Domino Data directory back to the directory
defined
   in Notes.ini (e.g. /local/notesdata)
4. Restore all archived transaction logs to the directory
defined
   in Notes.ini (e.g. /local/notesdata/logdir)

Continue ? (Y) or (N) y

Running media recovery ...
directory /local/notesdata// already exists
Please wait, creating new transaction logs in directory:
/local/notesdata/logdir/
02/01/2007 11:38:43 AM  Recovery Manager: Restart Recovery
complete. (0/0 databases needed full/partial recovery)
02/01/2007 11:38:45 AM  Recovery Manager: Assigning new DBIID
```

```
for /local/notesdata/names.nsf (need new backup for media
recovery).
Media Recovery Replay (0 MB): 100%
02/01/2007 11:38:45 AM  Recovery Manager: Media Recovery
complete for /local/notesdata/dfc/dfc100.nsf, last update
applied .

 Backup file /local/notesdata/dfc/dfc100.nsf recovered.
Media Recovery Replay (0 MB): 100%
02/01/2007 11:38:46 AM  Recovery Manager: Media Recovery
complete for /local/notesdata/help/decsdoc.nsf, last update
applied .

…

 Backup file /local/notesdata/iNotes/help70_iwa_en.nsf
recovered.
Media Recovery Replay (0 MB): 100%
02/01/2007 11:38:50 AM  Recovery Manager: Media Recovery
complete for /local/notesdata/mail/notes.nsf, last update
applied .

 Backup file /local/notesdata/mail/notes.nsf recovered.
bash-3.00$
```

10. Restart the Lotus Domino services.

Restore a single database

To restore a single database:

5. Place the restored database file to the original directory path:

   Database and archived transaction logs are stored on OBS along with their full path information, place them back to their original location (location where the backup was originally performed).

6. *Optional for media recovery* - Place the restored archived transaction logs to their original directory path.

7. In the OBM installation bin folder, open "DominoRecover.bat" with a text editor.

   Modify the User Defined Section according to your setup.

   For example, to recover database "admin4.nsf", with the backed up data was restored to directory path - /restore/local/notesdata

DominoRecover.sh:

```
###############  Start: User Defined Section  ##############
```

```
# ---------------------- DATA_DIR ----------------------
# | The Domino directory which contains notes.ini,      |
# | the Domino databases, and templates.                |
# | e.g. DATA_DIR=/local/notesdata                      |
# -------------------------------------------------------
DATA_DIR=/local/notesdata

# ---------------------- LOTUS ----------------------
# | The directory in which all Lotus products for     |
# | UNIX are installed.                               |
# | e.g. LOTUS=/opt/ibm/lotus                         |
# -----------------------------------------------------
LOTUS=/opt/ibm/lotus

# ---------------------- INPUT_FILE ----------------------
# | The path to an input file if you want to restore    |
# | one database only. If you want to restore all       |
# | databases, leave INPUT_FILE blank.                  |
# -------------------------------------------------------
SET INPUT_FILE=/restore/local/notesdata/admin4.nsf

# ---------------------- RESTOREDB ----------------------
# | The path to a database file if you want to          |
# | restore one database only. If you want to restore   |
# | all databases, leave RESTOREDB blank.               |
# -------------------------------------------------------
SET RESTOREDB=/local/notesdata/admin4.nsf

# ---------------------- RECDATE ----------------------
# | The year, month and day you want to recover         |
# | the database to. Set them according to the date     |
# | format set in your system.                          |
# | e.g. SET RECDATE=11/15/2006                         |
# | If you want to restore all databases, leave         |
# | RECDATE blank.                                      |
# | e.g. SET RECDATE=                                   |
# -------------------------------------------------------
SET RECDATE=18/01/2007

# ---------------------- RECTIME ----------------------
# | The time in hour and minute you want to recover the
# | database to. Set them according to the time format
# | set in your system.
# | e.g. SET RECTIME=13:00
# | If you want to restore all databases, leave RECTIME
# | blank.
# | e.g. SET RECTIME=
# -------------------------------------------------------
SET RECTIME=22:41
```

8. Save, and execute the "DominoRecover.sh" script file afterward.

```
>usr/local/obm/bin/DominoRecover.sh
```

Important:
Please ensure that you are running as the Domino user (e.g. notes)

Media recovery is performed for the individual database.

Content of the database will be restored to the last committed transaction found in the archived transaction log

Example:

Media Recovery Example:

```
bash-3.00$ cd /usr/local/obm/bin
bash-3.00$ ./DominoRecover.sh
Media Recovery Utility for Lotus Domino 5.0 or above

directory /local/notesdata// already exists

 Recovering backup file ...

Restart Analysis (0 MB): 100%
18/01/2007 03:35:56 PM  Recovery Manager: Restart Recovery
complete. (0/0 databases needed full/partial recovery)
Media Recovery Replay (1 MB): 30% 50% 80% 100%
18/01/2007 03:35:57 PM  Recovery Manager: Media Recovery
complete for /local/restore/local/notesdata/admin4.nsf, last
update applied .

 Backup file /local/restore/local/notesdata/admin4.nsf
recovered.

 Taking database /local/notesdata/admin4.nsf offline ...


 Restoring database /local/notesdata/admin4.nsf
  from recovered backup file
/local/restore/local/notesdata/admin4.nsf ...
Database file /local/notesdata/admin4.nsf restored from
/local/restore/local/not esdata/admin4.nsf

 Bringing database /local/notesdata/admin4.nsf online ...


Program completed successfully.
```

9. Restart the Lotus Domino services.

20 Backup / Restore MySQL Server

This chapter describes in details how to backup and restore MySQL server with OBM.

20.1 Supported versions

The MySQL backup module is supported for the following MySQL versions:

- MySQL 5.1
- MySQL 5.5.15

For more details, please refer to Help Centre Article:
https://help..com/openArticle.aspx?aid=2323

20.2 Requirements and recommendations

Please ensure that the following requirements are met by the MySQL server.

1. OBM is installed on the MySQL server.

2. Data selected for backup will be temporarily spooled to a temp directory before being uploaded to the backup server

   Please ensure that the temporary directory configured for the backup have sufficient disk space for the backup operation.

3. A MySQL user with *ALL PRIVILEGES* must be prepared for the backup operation.

   For example:

```
mysql> GRANT ALL PRIVILEGES ON *.* TO
'username'@'localhost' IDENTIFIED BY 'password';

mysql> GRANT ALL PRIVILEGES ON *.* TO
'username'@'localhost.localdomain' IDENTIFIED BY
'password';

mysql> FLUSH PRIVILEGES;
```

4. The 'information_schema' database is a virtual system database, which contains information about the user databases on the MySQL instance.

   It is read-only and cannot be backed up.

20.3 Overview

The following steps are performed during a backup job:

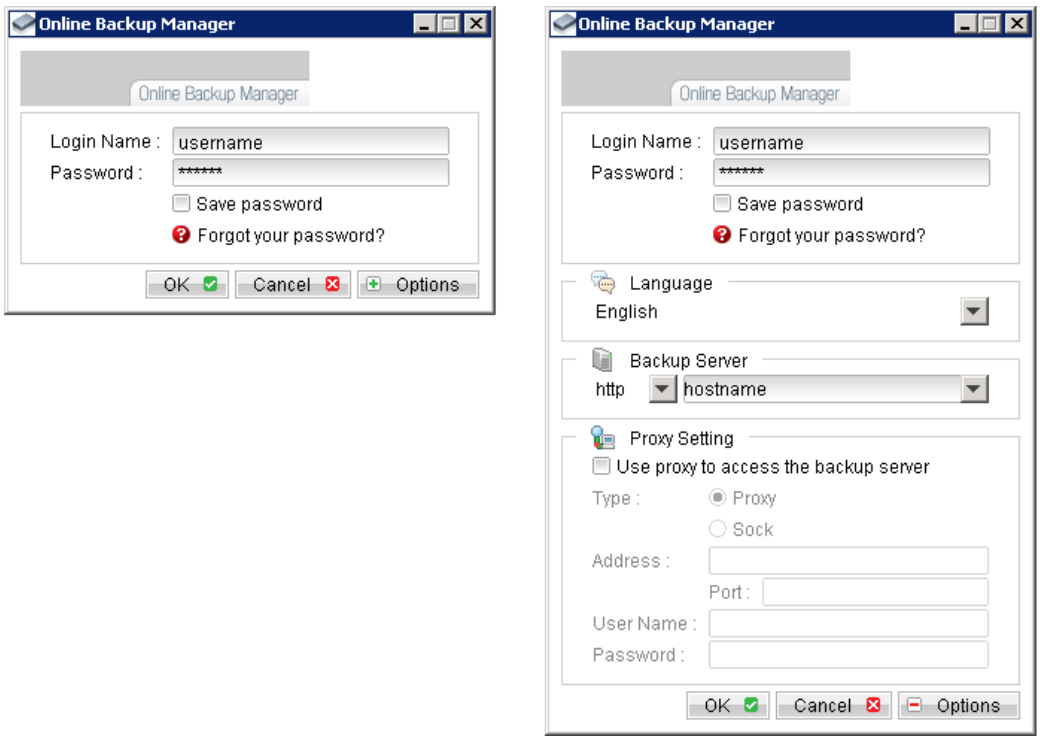
1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Database (including stored routines) are backed up to the temporary spool path.
4. Server and local file lists are compared to determine which file will be uploaded.
5. Delta file is generated for modified file (if necessary).
6. Data are removed from the temporary spool path.
7. Backup completed successfully.

20.4 How to backup MySQL server (Windows)

Refer to the following instructions to backup MySQL database installation on Windows:

1. Login to the backup application's user interface.

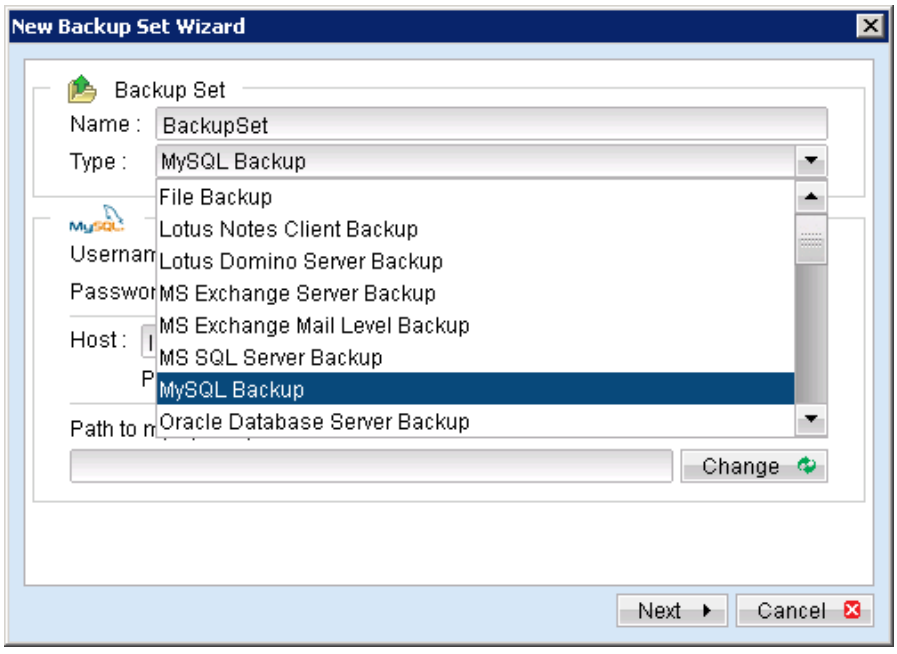
   Double-click on the OBM desktop icon or right-click on the system tray icon:



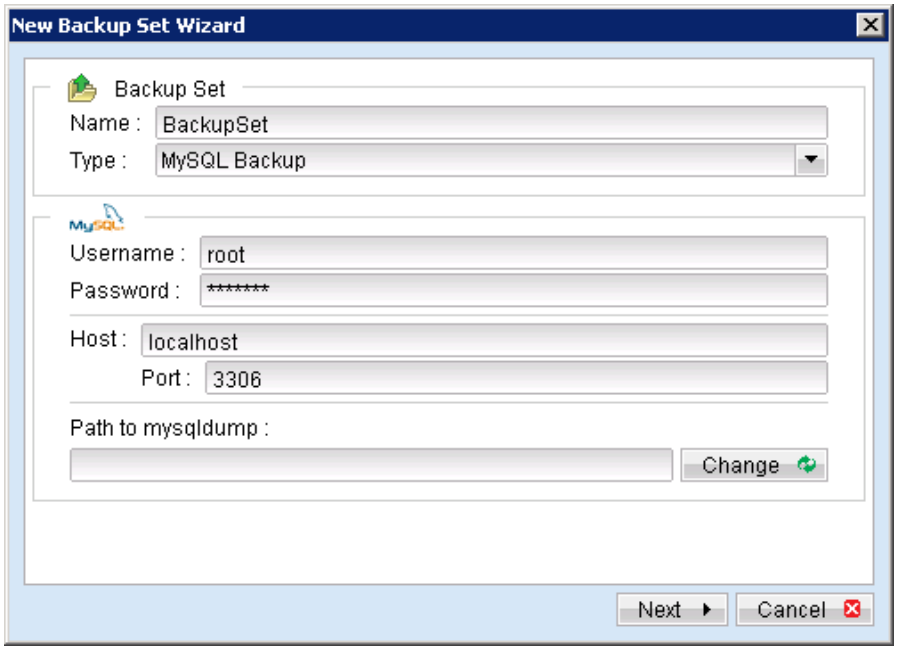
Note:
OBM must be installed on the MySQL server.

2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

3. Create a MySQL Backup set by selecting [MySQL Backup] from the backup set type dropdown menu.



4. Enter the corresponding information required:



Menu Items	Description
Name	Enter a backup set name of your choice.
Type	Select backup set type [MySQL Backup].
Username	Enter the username of the MySQL account with all privileges.
Password	Enter the username of the MySQL account with all privileges.
Host	Enter the IP address or hostname of the MySQL database server. Note: OBM must be installed on the MySQL database server
Port	Enter the TCP/IP port for accessing the MySQL database server (default: 3306).
Path to mysqldump	Enter the directory path of mysqldump. Default location is: ${MySQL-Install-Home}\bin

5. Select [Next] to proceed.

6. In the backup source selection screen, select the databases for backup.

Important:
Do not select the 'information_schema' database for backup, it is a read-only database and cannot be backed up.

7. Configure a backup schedule for unattended backups.

   Note:
   Multiple backup schedules of different types can be configured for the same backup set.

8. Select an encryption setting for your backup set.

9. Press the [OK] button to complete the configuration of backup set.

10. Scheduled backup will run automatically at the configured schedule time.

11. Click [Backup] button on the left panel to perform a backup immediately.

20.5 How to backup MySQL server (Linux)

Refer to the following instructions to backup MySQL database installation on Linux:

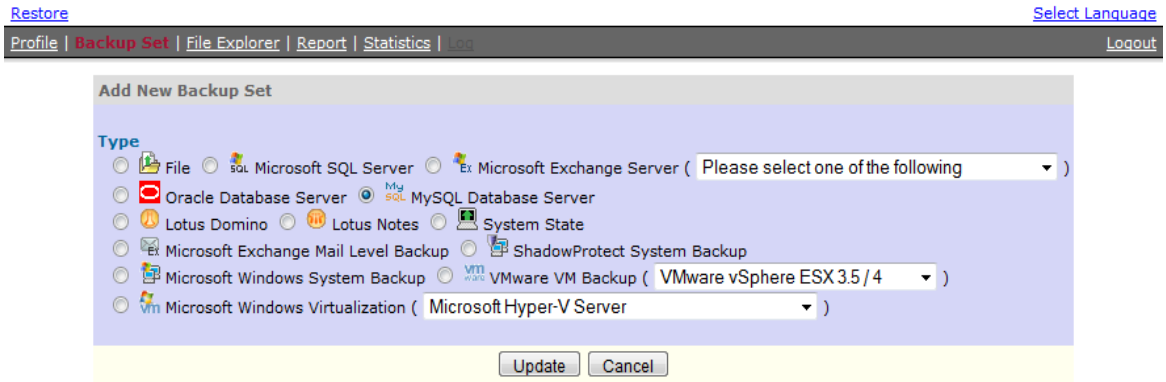
1. Install OBM on the MySQL database server.

   Note:
   OBM must be installed on the MySQL database server

2. Create a new MySQL backup set on the web interface.

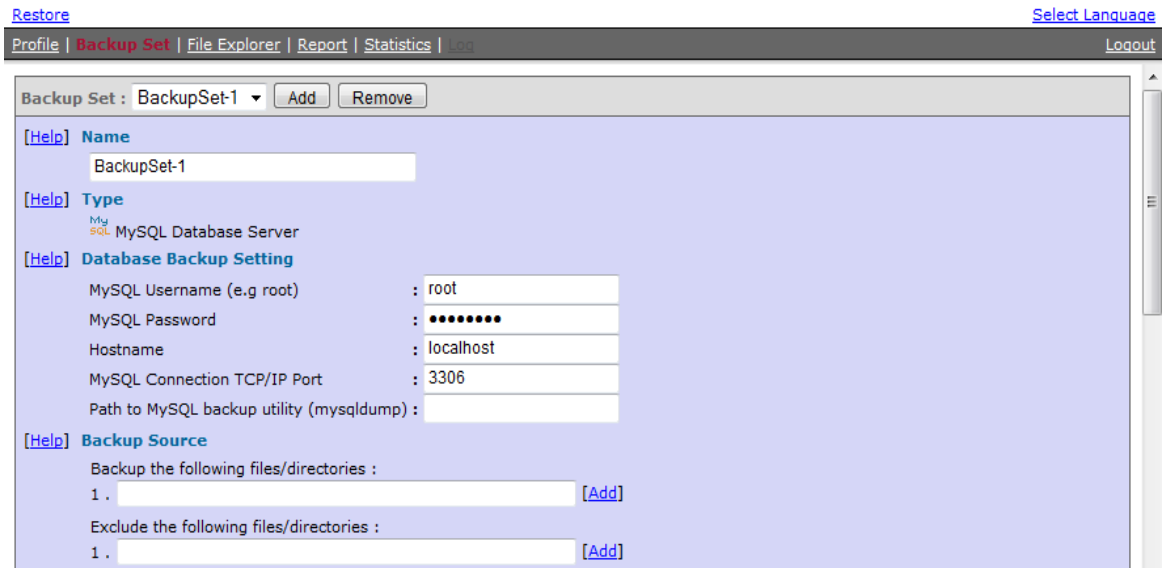
3. Login to the OBS web console, select [Backup Set].

4. Press the [Add] button to access the Add New Backup Set menu.



5. Select the [MySQL Database Server] radio button and [Update].

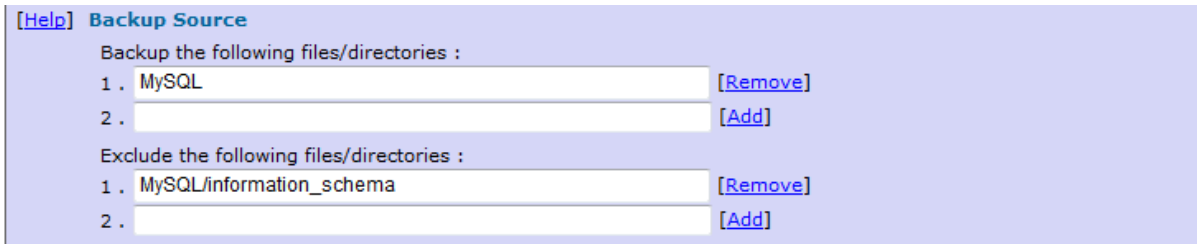
6. Enter the Name and Database Backup Setting required:



Menu Items	Description
Name	Enter a backup set name of your choice.
MySQL Username	Enter the username of the MySQL account with all privileges.
MySQL Password	Enter the username of the MySQL account with all privileges.
Hostname	Enter the IP address or hostname of the MySQL database server. Note: OBM must be installed on the MySQL database server
MySQL Connection TCP/IP Port	Enter the TCP/IP port for accessing the MySQL database server (default: 3306).
Path to MySQL backup utility (mysqldump)	Enter the directory path of mysqldump. Default location is: ${MySQL-Install-Home}\bin

7. Enter the Backup Source required:

   To backup all databases, enter "MySQL" in the [Backup the following files/directories] field:



   To backup or exclude individual database, enter "MySQL/Database_Name".

   Important:
   The 'information_schema' database is a read-only database and cannot be backed up

8. Configure a backup schedule for unattended backups.

   Note:
   Multiple backup schedules of different types can be configured for the same backup set.

9. Press the [Update] button to save the newly created backup set.

10. Login to the MySQL database server with OBM installed.

11. Start the Configurator.sh script by accessing the backup client installation bin folder:

```
>sh OBM_HOME/bin/Configurator.sh
```

12. Follow the instructions provided in the Configurator to complete the configuration of the backup set.

    Note:
    For Linux with GUI installed, you can also create a backup set via the OBM user interface (similar to the procedures provided in the Windows section).

    Launch the OBM user interface:

```
>sh OBM_HOME/bin/RunOBC.sh
```

13. Scheduled backup will run automatically at the configured schedule time.

14. To perform a backup immediately, execute the RunBackupSet.sh script with the backup set name or ID:

```
>sh OBM_HOME/bin/RunBackupSet.sh BackupSet_Name
```

    Important:
    Before executing the script, please edit the BACKUP_TYPE parameter within the RunBackupSet.sh script file from -

    BACKUP_TYPE="FILE"

    to

    BACKUP_TYPE="DATABASE"

20.6 How to restore MySQL server

Refer to the follow instructions to restore MySQL database for both installation on Windows and Linux.

1. Install OBM on the MySQL database server (if required).
2. Restore the MySQL database file from backup; restore the database backup files from the OBS server (e.g. db_name.sql)
3. For restore of a non-existing database, first create the database:
   - Connect to the MySQL Server.

```
>mysql
```

   - Create the database to be restored.

```
mysql> CREATE DATABASE IF NOT EXISTS db_name
```

4. Restore the database backup file back into the MySQL server.

```
mysql> USE db_name;

mysql> SOURCE db_name.sql;
```

   Note:
   You may need to specify the full directory path for "db_name.sql" in the above command.

5. Repeat the same procedure for each database to be restored.

21 Email Reporting

OBM users are kept informed with the status of their backup activities via email reports.

Please ensure that a valid email address is configured on the web console in order to receive the reports described in the following sections.

Note:
Availability of the following reports may be service provider dependent. If a report is not available, please check with your service provider for further details and availability.

21.1 New User Report

When a new backup account is created, a welcome email will be sent to the contact email address of the account.

A welcome email contains the following information:

Sample

Welcome to Online Backup Services
Generated at: Thu Jan 19 17:57:23 GMT+08:00 2012
Getting started:
Please follow the instructions available in the installation wizard to download and install OBM.
Further Information:
If further assistance is required, please refer to the FAQs.
User Setting
Login Name :user-name
Alias :
Language :English
Contact :username@ex2k10.bsp.test
Backup Quota :50G

Key	Description
Login Name	**Login name of the backup account.**
Alias	**Alias of the backup account.**
Language	**Preferred language of the backup account.**
Contact	**Email address of the backup account.**
Backup Quota	**Backup quota allocated for the backup account.**

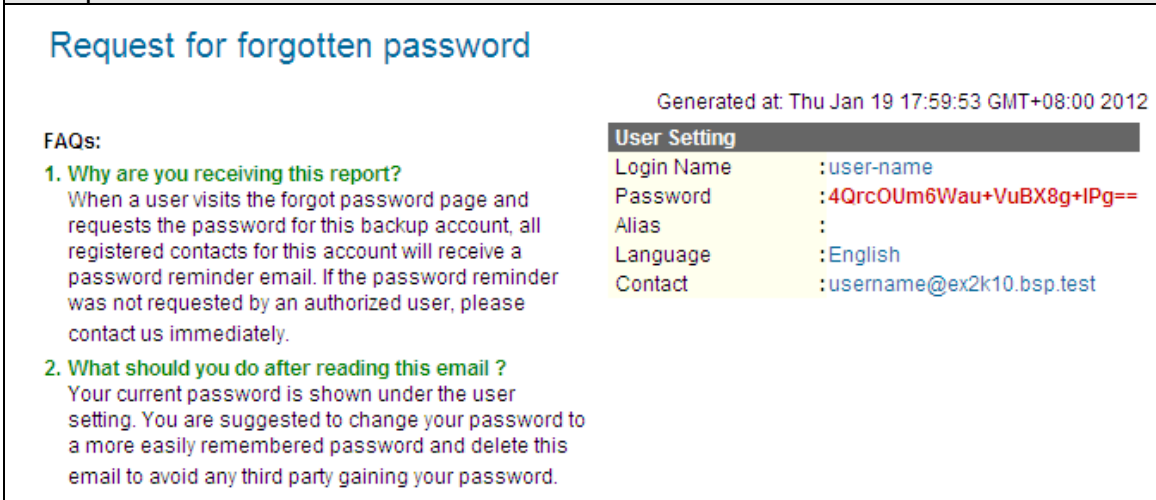
21.2 Forgot Password Report

User can retrieve his or her password by requesting the forgotten password email via the web console [Forgotten your password].

An email will be sent to the backup account email address with the password in hashed format.

A request forgotten password email contains the following information:

Sample


Request for forgotten password
Generated at: Thu Jan 19 17:59:53 GMT+08:00 2012
FAQs:
1. Why are you receiving this report?
When a user visits the forgot password page and requests the password for this backup account, all registered contacts for this account will receive a password reminder email. If the password reminder was not requested by an authorized user, please contact us immediately.
2. What should you do after reading this email ?
Your current password is shown under the user setting. You are suggested to change your password to a more easily remembered password and delete this email to avoid any third party gaining your password.
User Setting
Login Name :user-name
Password :4QrcOUm6Wau+VuBX8g+IPg==
Alias :
Language :English
Contact :username@ex2k10.bsp.test

Key	Description
Login Name	**Login name of the backup account.**
Password	**Password of the backup account in hashed format.** **Note:** **The hashed password can be used to login to the OBM user interface, where the user will be prompted to change the password.**
Alias	**Alias of the backup account.**
Language	**Preferred language of the backup account.**
Contact	**Email address of the backup account.**

21.3 Backup Job Report

Backup job report is sent to the corresponding backup account after each backup job performed.

The report is sent on the 57th minute of every hour by a system routine job, for all jobs performed during that hour.

A backup job report email contains the following information:

Sample

Online Backup Job Report - BackupSet

Generated at:Thu Jan 19 23:18:30 GMT+08:00 2012

Backup Job Summary

Backup Time	:2012/01/19 17:59 - 2012/01/19 17:59
Job Status	:Backup finished successfully
New Files*	:30 [8.44M]
Updated Files*	:0 [0]
Updated Access Permissions*	:0 [0]
Deleted Files*	:0 [0]
Moved Files*	:0 [0]
Copied Files*	:0 [0]

* Unit = No of files [Total file size]

A full listing of all backup files is available in the attached file.

User Setting

Login Name	:user-name
Alias	:
Language	:English
Contact	:username@ex2k10.bsp.test

Backup Setting

Backup Source	:C:\Backup Source But exclude the following: C:\Backup Source\Test.doc C:\Backup Source\Test1.doc

Backup Statistics

Data Area**	: 30 [8.44M / 12.08M]
Retention Area**	: 0 [0 / 0]
Backup Quota	: 50G
Remaining Quota	: 49.99G

** Unit = No of files [Total file zipped size / Total file size]

FAQs:

1. Why are you receiving this report?
   You are receiving this report because you are registered as one of the contacts of this Online Backup account and this particular account has performed a backup job recently.
2. What if you have exceeded your quota?
   If your retention area is not empty, you can empty your retention area to free up more space. Please contact us for more information on how to increase your storage quota.

If further assistance is required, please refer to the FAQs.

Key	Description
Backup Job Summary	
Backup Time	**The time when the backup job ran.**
Job Status	**The overall status of the backup job:** • **Backup finished successfully** • **Backup finished with error** • **Backup finished with warning**

	• **Backup interrupted by system** • **Backup interrupted by user**
New Files	**Total number and size of new files uploaded.**
Updated Files	**Total number and size of updated files uploaded.**
Updated Access Permissions	**Total number and size of permission updated files uploaded.**
Deleted Files	**Total number and size of files deleted.**
Moved Files	**Total number and size of files relocated.**
Copied Files	**Total number and size of files copied.**
User Setting	
Login Name	**Login name of the backup account.**
Alias	**Alias of the backup account.**
Language	**Preferred language of the backup account.**
Contact	**Email address of the backup account.**
Backup Setting	
Backup Source	**Backup source selected for the job.**
Backup Statistics	
Data Area	**Total number and size of files stored in the data area.**
Retention Area	**Total number and size of files stored in the retention area.** **Previous copies of updated or deleted backup files are retained in the retention area according to the retention policy configured for the backup set.**
Backup Quota	**Backup quota allocated for the account.**
Remaining Quota	**Remaining quota of the account.**

A full backup job report, containing a listing of all files backed up by the corresponding job, is also attached to the email in zipped format.

A full backup job report email contains the following information:

Sample

Full Backup Report

Generated at: Thu Jan 19 23:18:30 GMT+08:00 2012

Backup Job Summary	
Login Name	user-name
Backup Set	BackupSet (1326967067630)
Backup Job	2012-01-19 (17:58)
Job Status	Backup finished successfully
Backup Time	2012/01/19 17:59 - 2012/01/19 17:59 (HKT)

Backup Job Statistics	
New Files*	2 [8.4M / 12.1M (30%)]
Updated Files*	0 [0 / 0 (0%)]
Permission Updated Files*	0 [0 / 0 (0%)]
Deleted Files*	0 [0 / 0 (0%)]
Moved Files*	0 [0 / 0 (0%)]
Copied Files*	0 [0 / 0 (0%)]

* Unit = No of files [Total file zipped size / Total file size (ratio)]

Backup Logs

No.	Type	Timestamp	Backup Logs
1	Info	2012/01/19 17:59	Start [Windows XP (Ahsay), AhsayOBM 6.7.0.0]
2	Info	2012/01/19 17:59	Using Temporary Directory C:\Documents and Settings\temp
3	Info	2012/01/19 17:59	Start running pre-commands
4	Info	2012/01/19 17:59	Finished running pre-commands
5	Info	2012/01/19 17:59	Start creating Shadow Copy Set ...
6	Info	2012/01/19 17:59	Shadow Copy Set successfully created
7	Info	2012/01/19 17:59	Deleting Shadow Copy snapshot for volume "C:\"
8	Info	2012/01/19 17:59	Start running post-commands
9	Info	2012/01/19 17:59	Finished running post-commands

New Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
1	C:\	1.5k / 0 [0%]	-
2	C:\Backup Source	1.5k / 0 [0%]	-
3	C:\Backup Source\FolderA	1.5k / 0 [0%]	-
4	C:\Backup Source\FolderB	1.5k / 0 [0%]	-
5	C:\Backup Source\FolderB\Test.doc	2.6k / 10.5k [75%]	2011/07/25 09:54
6	C:\Backup Source\FolderA\Test.doc	2.6k / 10.5k [75%]	2011/07/25 09:54

Updated Files

No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been updated.			

Permission Updated Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No Permissions have been updated.			

Deleted Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No files have been deleted.			

Moved Files

No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been moved.			

Copied Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No files have been copied.			

Note: This report shows all information recorded for this backup job

Key:

Backup Logs	Information / Warning / Error logged in this backup job
New Files	Files added since last backup job. These files are now in the current data area.
Updated Files	Files updated since last backup job. These files are now in the current data area while the older version of the same files are now in the retention area.
Deleted Files	Files deleted since last backup job. These files are now in the retention area.
Moved Files	Files moved since last backup job. These file movements have been updated on the backup server.
Copied Files	Files that are copied from another file with same data in server. They are copied in server instead of being uploaded again.
[C]	Checksum file
[D]	Delta file

Key	Description
Backup Job Summary	
Login Name	**Login name of the backup account.**
Backup Set	**Name of the backup set.**
Backup Job	**Time of the backup job in the following format:** **Year-Month-Day (hour:minute)**
Job Status	**The overall status of the backup job:** • **Backup finished successfully** • **Backup finished with error** • **Backup finished with warning** • **Backup interrupted by system** • **Backup interrupted by user**
Backup Time	**Start and end time of the backup job.**
Backup Job Statistics	
New Files	**Total number and size of new files uploaded.**
Updated Files	**Total number and size of updated files uploaded.**
Permission Update Files	**Total number and size of permission updated files uploaded.**
Deleted Files	**Total number and size of files deleted.**
Moved Files	**Total number and size of files relocated.**
Copied Files	**Total number and size of files copied.**
Backup Logs	
Backup Logs	**Log messages of the backup operation.**
File List	
New File List	**List of all new files uploaded.**
Updated File List	**List of all updated files uploaded.**
Permission Updated File List	**List of all permission updated files uploaded.**

Deleted File List	**List of all files deleted.**
Moved File List	**List of all files relocated.**
Copied File List	**List of all files copied.**

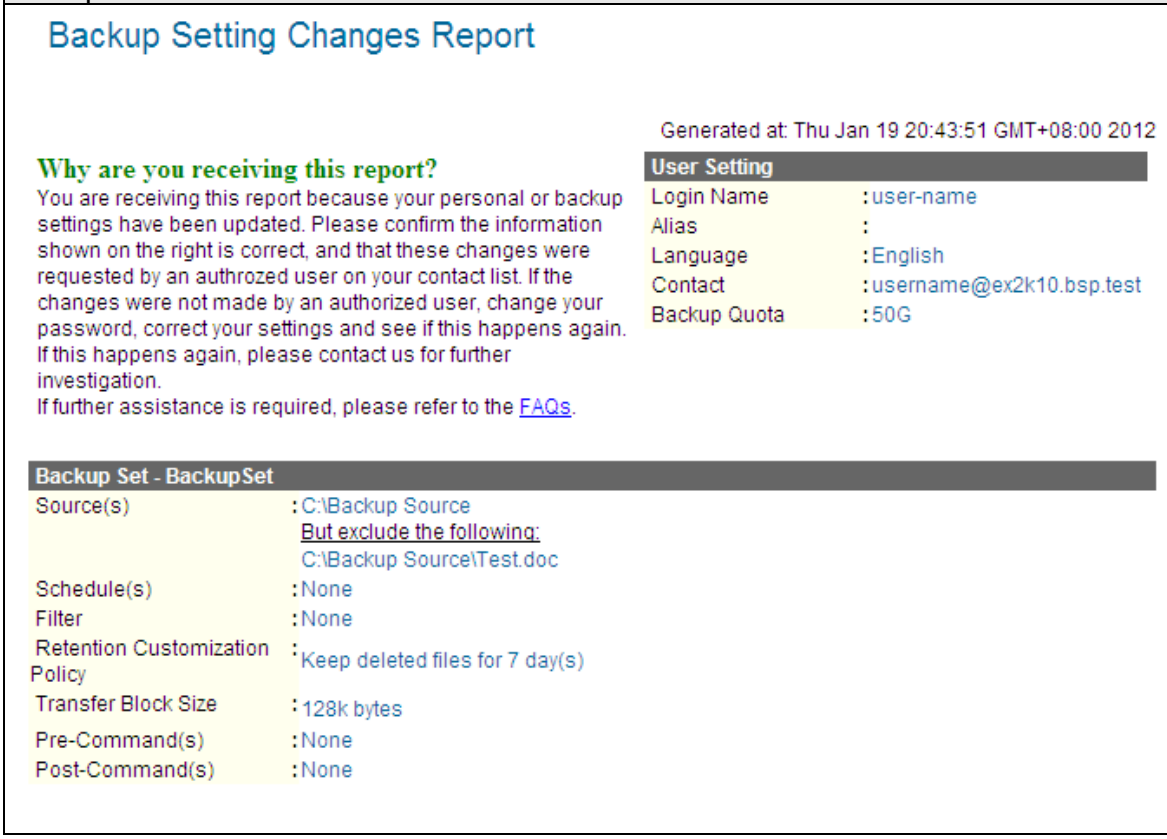
21.4 Setting Change Report

Setting change report is sent to the corresponding backup account after any setting change.

This report allows users to keep track of changes made to their backup account.

A backup setting changes report email contains the following information:

Sample


Backup Setting Changes Report
Generated at: Thu Jan 19 20:43:51 GMT+08:00 2012
Why are you receiving this report?
You are receiving this report because your personal or backup settings have been updated. Please confirm the information shown on the right is correct, and that these changes were requested by an authrozed user on your contact list. If the changes were not made by an authorized user, change your password, correct your settings and see if this happens again. If this happens again, please contact us for further investigation.
If further assistance is required, please refer to the FAQs.
User Setting
Login Name : user-name
Alias :
Language : English
Contact : username@ex2k10.bsp.test
Backup Quota : 50G
Backup Set - BackupSet
Source(s) : C:\Backup Source
But exclude the following:
C:\Backup Source\Test.doc
Schedule(s) : None
Filter : None
Retention Customization Policy : Keep deleted files for 7 day(s)
Transfer Block Size : 128k bytes
Pre-Command(s) : None
Post-Command(s) : None

Key	Description
User Setting	
Login Name	**Login name of the backup account.**
Alias	**Alias of the backup account.**
Language	**Preferred language of the backup account.**
Contact	**Email address of the backup account.**
Backup Quota	**Backup quota allocated for the backup account.**

Backup Set	
Source	**Backup source setting for the backup set.**
Schedule	**Backup schedule setting for the backup set.**
Filter	**Backup filter setting for the backup set.**
Retention Customization Policy	**Retention policy setting for the backup set.**
Transfer Block Size	**Transfer block size setting for the backup set.**
Pre-Command	**Pre-backup command setting for the backup set.**
Post-Command	**Post-backup command setting for the backup set.**

21.5 Inactive User Report

Inactive user report is sent to backup account inactive for more than 7 days.

The report serves as a reminder that no backup has been performed with this account for the specified period of time.

For trial account, the account may also be removed from the backup server automatically, depending on your service providers setting.

An inactive user report email contains the following information:

Sample

Inactive User Report
Generated at: Tue Aug 12 18:21:45 CST 2008
Why are you receiving this report?
You are receiving this report because this backup account has been inactive for 30 days. If this account stays inactive for another 30 days, this account will be removed from our system automatically without further notice. The following is the backup activity of this account:
Last Login Time : 2008-08-12 05:07:04 PM
Last Backup Time : 2008-08-12 05:02:04 PM
If further assistance is required, please refer to the FAQs section.
User Setting
Login Name :NewAccount
Alias :NewAccount Name
Language :English
Contact :new_account@your-company.com

Key	Description

Login Name	**Login name of the backup account.**
Alias	**Alias of the backup account.**
Language	**Preferred language of the backup account.**
Contact	**Email address of the backup account.**
Last Login Time	**Last login time of the backup account.**
Last Backup Time	**Last backup time of the backup account.**

22 Web Features

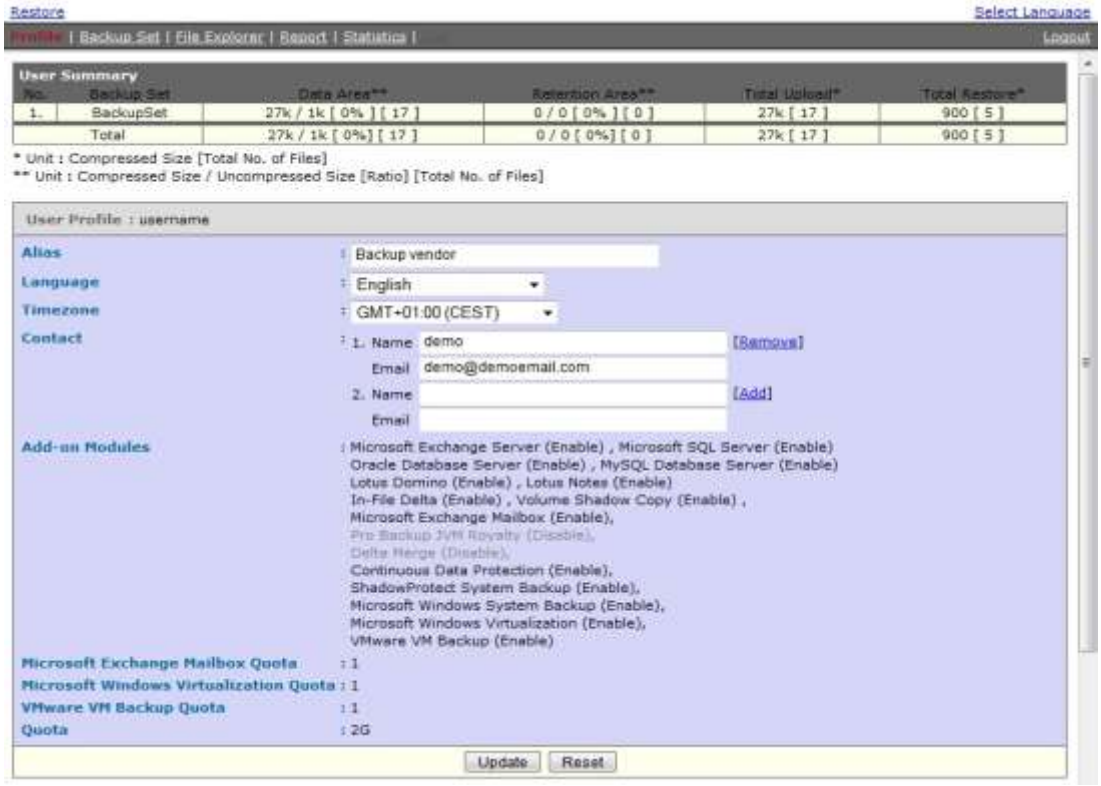
Other than the features of OBM described in previous chapters, the web interface of OBS provides you access to some additional features that are not available in OBM. This chapter describes each of these features in details.

22.1 Install OBM

Before you can use OBM, you have to download the OBM installer from the web interface of OBS and install OBM onto your computer. Please refer to the Installing OBM section for information on how to install OBM onto your computer.

22.2 Update User Profile

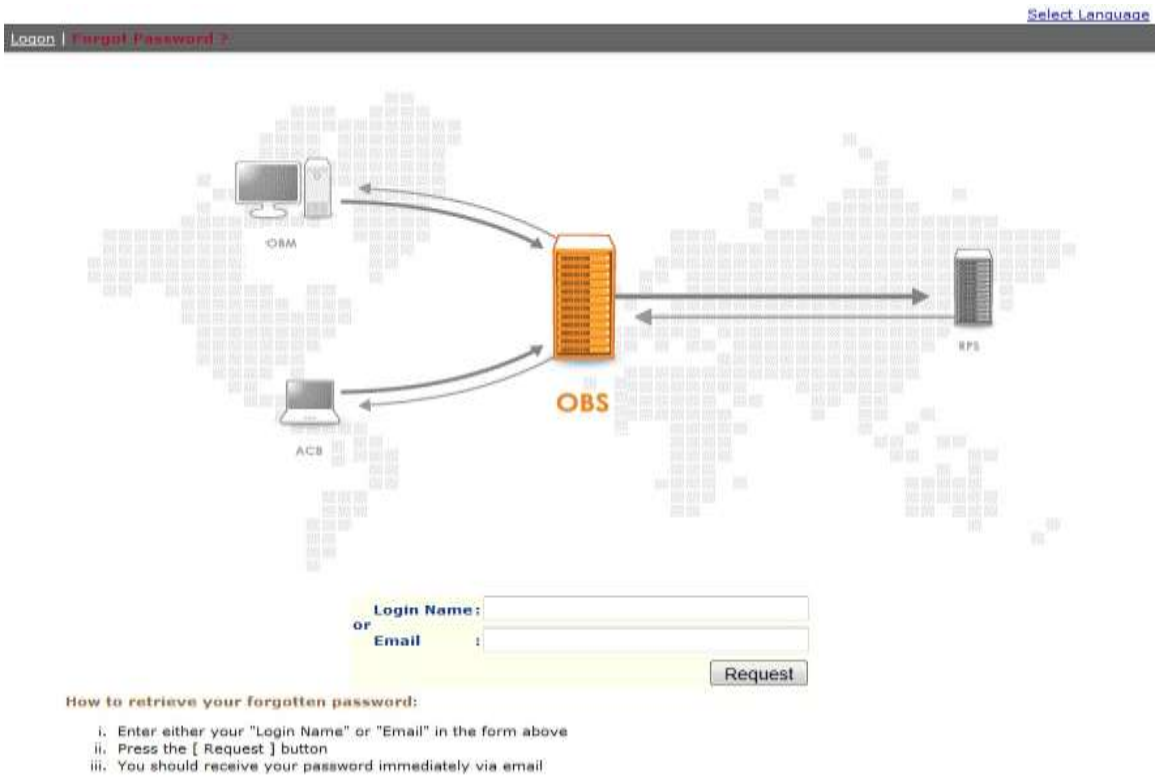
You can update your user profile by using the [Profile] panel available on the web interface. To change your profile, just make any changes to your profile on the panel shown below and press the [Update] button.


Restore
Select Language
Profile | Backup Set | File Explorer | Report | Statistics |
Logout
User Summary
No. Backup Set Data Area** Retention Area** Total Upload* Total Restore*
1. BackupSet 27k / 1k [0%] [17] 0 / 0 [0%] [0] 27k [17] 900 [5]
Total 27k / 1k [0%] [17] 0 / 0 [0%] [0] 27k [17] 900 [5]
* Unit : Compressed Size [Total No. of Files]
** Unit : Compressed Size / Uncompressed Size [Ratio] [Total No. of Files]
User Profile : username
Alias : Backup vendor
Language : English
Timezone : GMT+01:00 (CEST)
Contact : 1. Name demo [Remove]
Email demo@demoemail.com
2. Name [Add]
Email
Add-on Modules : Microsoft Exchange Server (Enable) , Microsoft SQL Server (Enable)
Oracle Database Server (Enable) , MySQL Database Server (Enable)
Lotus Domino (Enable) , Lotus Notes (Enable)
In-File Delta (Enable) , Volume Shadow Copy (Enable) ,
Microsoft Exchange Mailbox (Enable),
Pre Backup JVM Royalty (Disable),
Delta Merge (Disable),
Continuous Data Protection (Enable),
ShadowProtect System Backup (Enable),
Microsoft Windows System Backup (Enable),
Microsoft Windows Virtualization (Enable),
VMware VM Backup (Enable)
Microsoft Exchange Mailbox Quota : 1
Microsoft Windows Virtualization Quota : 1
VMware VM Backup Quota : 1
Quota : 2G
Update
Reset

Key	Description
Quota	**Backup quota**
Data Area	**Total number and size of backup files stored in the data area.**
Retention Area	**Total number and size of backup files stored in the retention area.**
Total Upload	**Total number and size of backup files uploaded to the backup server.**
Total Restore	**Total number and size of backup files restored from the backup server.**
Login Name	**Login name.**
Alias	**Display Name of your backup account.**
Language	**Preferred Language for your backup report.**
Time Zone	**Your Time zone.**
Contact	**Email Address that will be used to contact you.**

22.3 Request Forgotten Password

If you have forgotten your password, you can retrieve it by simply entering your login name or your registered email address on the [Password Request] form and press the [Request] button. Your password will be sent to your registered email address automatically.



22.4 Restore / Delete / Undelete Backup Files

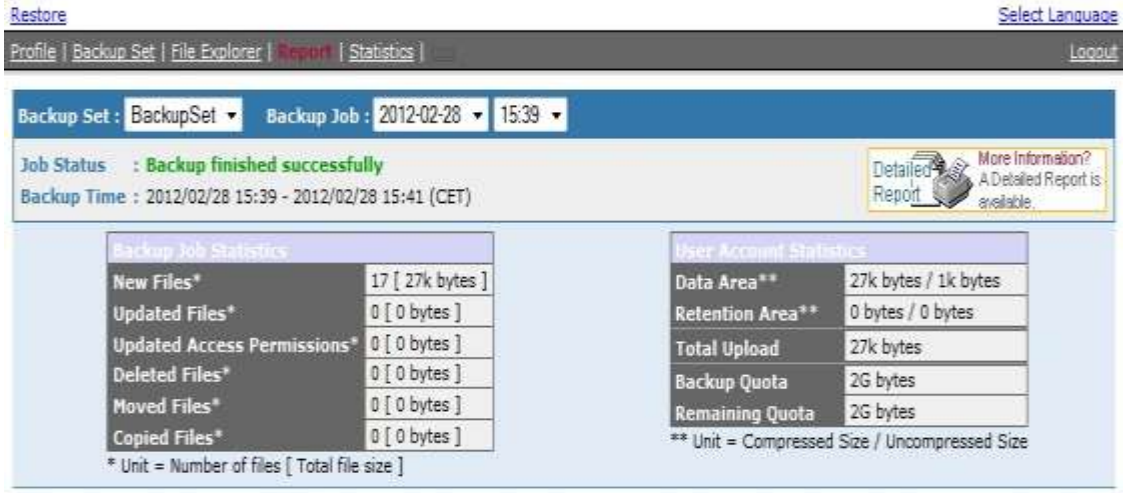
Using the [File Explorer], you can browse through the backup data (both current and previous versions) on OBS. You can select any current backup files to Restore or Delete. You can also select any deleted backup files (in gray) to Undelete.

Important:
Restore of native features, e.g. file attribute / permission / symbolic links / junction points are not supported by the Web Restore Applet.

Restore
Select Language
Profile | Backup Set | File Explorer | Report | Statistics |
Logout
Rows/Page: 50
Home > BackupSet > C:\ > Documents and Settings > Tester > Favorites > Links
Show files As Of 2012-02-29 Latest Show all files Show Jobs View
Show Advanced Option
Restore Delete
File / Directory
Size
Last Modified
Zipped [Ratio]
..
Suggested Sites.url 302 2012/02/28 10:59 244 [19%]
Web Slice Gallery.url 226 2012/02/28 10:58 212 [6%]
desktop.ini 84 2012/02/28 10:58 148 [0%]
Restore Delete
Note:
1. This shows all files / directories within a backup job of a backup set.
2. Files shown in light gray color are retained in the retention area.
3. To restore files/directories, please click the [Restore] button shown above.
4. To delete files/directories, please click the [Delete] button shown above.
5. [D] = Differential delta file
6. [I] = Incremental delta file
7. Size (number): The number in the round bracket is the file size of delta file and it is not available for full file

22.5 Review Backup Jobs

In addition to reviewing your backup activities from the email report and from OBM, you can also review any of your backup jobs by using the [Report] panel available on the web interface. To review a backup job, select the required backup job from the [Backup Set] and [Backup Job] drop-down lists.

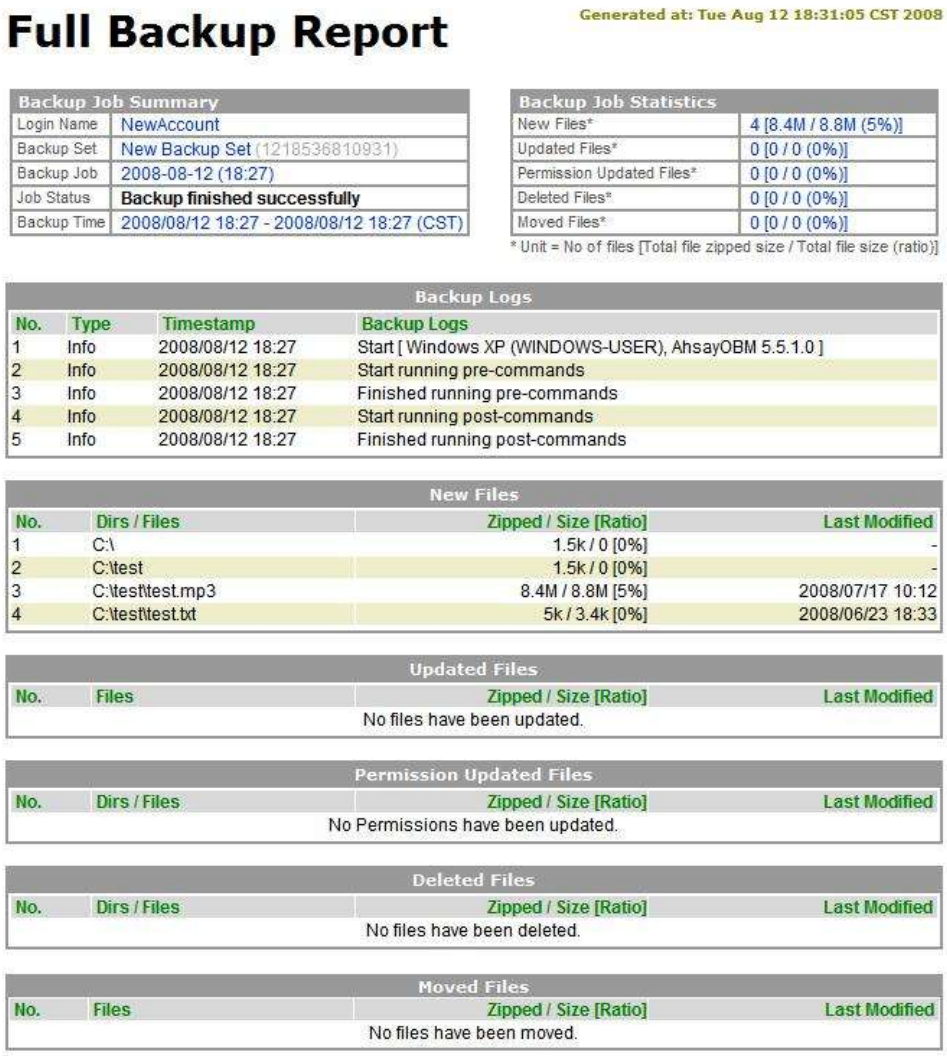

Restore
Select Language
Profile | Backup Set | File Explorer | Report | Statistics |
Logout
Backup Set : BackupSet
Backup Job : 2012-02-28 15:39
Job Status : Backup finished successfully
Backup Time : 2012/02/28 15:39 - 2012/02/28 15:41 (CET)
Detailed Report
More Information?
A Detailed Report is available.
Backup Job Statistics
New Files* 17 [27k bytes]
Updated Files* 0 [0 bytes]
Updated Access Permissions* 0 [0 bytes]
Deleted Files* 0 [0 bytes]
Moved Files* 0 [0 bytes]
Copied Files* 0 [0 bytes]
* Unit = Number of files [Total file size]
User Account Statistics
Data Area** 27k bytes / 1k bytes
Retention Area** 0 bytes / 0 bytes
Total Upload 27k bytes
Backup Quota 2G bytes
Remaining Quota 2G bytes
** Unit = Compressed Size / Uncompressed Size

Key	Description
Job Status	**The overall status of the backup job. Normally, you should see "Backup finished successfully" in this field. If you happen to get something else, please click the [Detailed Report] image on the page.**
Backup Time	**The time when the backup job ran.**
New Files	**Total number and size of backup files added to your backup set.**
Updated Files	**Total number and size of backup files updated in your backup set.**
Updated Access Permissions	**Total number and size of backup files with file permission updated in your backup set.**
Deleted Files	**Total number and size of backup files deleted from your backup set.**
Moved Files	**Total number and size of backup files relocated in your backup set.**
Copied Files	**Total number and size of backup files copied to another location in your backup set.**
Data Area	**The total backup data stored in the data area.**
Retention Area	**The total backup data stored in the retention area. Old copies of updated or deleted backup files are retained**

	in the retention area for the number of days as specified by the retention policy of the backup set before they are removed from the system
Total Upload	**Total number and size of backup files uploaded to the backup server.**
Backup Quota	**Backup Quota**
Remaining Quota	**Remaining Quota**

You can open the [Full Backup Report] to review all information logged by a backup job by clicking the [Detailed Report] image on the [Report] panel.

Full Backup Report



Full Backup Report

Generated at: Tue Aug 12 18:31:05 CST 2008

Backup Job Summary	
Login Name	NewAccount
Backup Set	New Backup Set (1218536810931)
Backup Job	2008-08-12 (18:27)
Job Status	Backup finished successfully
Backup Time	2008/08/12 18:27 - 2008/08/12 18:27 (CST)

Backup Job Statistics	
New Files*	4 [8.4M / 8.8M (5%)]
Updated Files*	0 [0 / 0 (0%)]
Permission Updated Files*	0 [0 / 0 (0%)]
Deleted Files*	0 [0 / 0 (0%)]
Moved Files*	0 [0 / 0 (0%)]

* Unit = No of files [Total file zipped size / Total file size (ratio)]

Backup Logs

No.	Type	Timestamp	Backup Logs
1	Info	2008/08/12 18:27	Start [Windows XP (WINDOWS-USER), AhsayOBM 5.5.1.0]
2	Info	2008/08/12 18:27	Start running pre-commands
3	Info	2008/08/12 18:27	Finished running pre-commands
4	Info	2008/08/12 18:27	Start running post-commands
5	Info	2008/08/12 18:27	Finished running post-commands

New Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
1	C:\	1.5k / 0 [0%]	-
2	C:\test	1.5k / 0 [0%]	-
3	C:\test\test.mp3	8.4M / 8.8M [5%]	2008/07/17 10:12
4	C:\test\test.txt	5k / 3.4k [0%]	2008/06/23 18:33

Updated Files

No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been updated.			

Permission Updated Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No Permissions have been updated.			

Deleted Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No files have been deleted.			

Moved Files

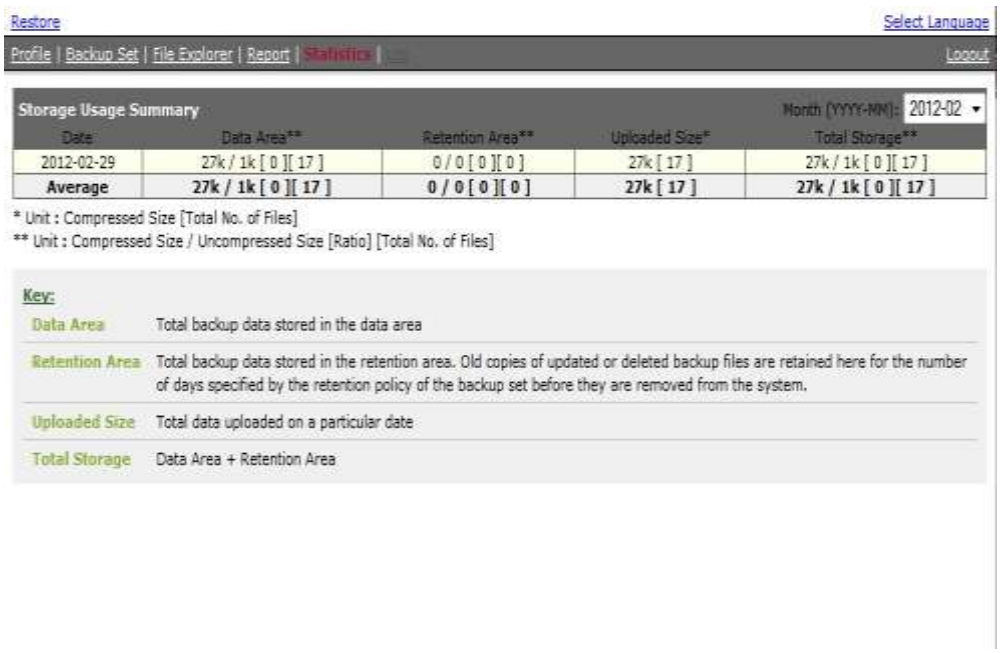
No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been moved.			

Key	Description
Login Name	**The login name of the user.**
Backup Set	**The name of the backup set.**
Backup Job	**The name of the backup job (which is the start time of the backup job).**

Job Status	**The overall status of the backup job.**
Backup Time	**The time when the backup job ran.**
Backup Logs	**All messages logged when running this backup job.**
New Files	**Total number and size of backup files added to your backup set.**
Updated Files	**Total number and size of backup files updated in your backup set.**
Permission Updated Files	**Total number and size of backup files with file permission updated in your backup set.**
Deleted Files	**Total number and size of backup files deleted from your backup set.**
Moved Files	**Total number and size of backup files relocated in your backup set.**
Copied Files	**Total number and size of backup files copied to another location in your backup set.**
New File List	**Full list of all backup files added to your backup set.**
Updated File List	**Full list of all backup files updated in your backup set.**
Permission Updated File List	**Full list of all backup files with file permission updated in your backup set.**
Deleted File List	**Full list of all backup files deleted from your backup set.**
Moved File List	**Full list of all backup files relocated in your backup set.**
Copied File List	**Full list of all backup files copied to another location in your backup set.**

22.6 Review Storage Statistics

You can review the amount of data you have stored on the backup server and uploaded to the backup server on each day by opening the [Statistics] panel available on the web interface. To review your storage statistics for a different month, just select the month from the [Month] drop-down list.


Restore
Select Language
Profile | Backup Set | File Explorer | Report | Statistics
Logout
Storage Usage Summary
Month (YYYY-MM): 2012-02
Date
Data Area**
Retention Area**
Uploaded Size*
Total Storage**
2012-02-29
27k / 1k [0][17]
0 / 0 [0][0]
27k [17]
27k / 1k [0][17]
Average
27k / 1k [0][17]
0 / 0 [0][0]
27k [17]
27k / 1k [0][17]
* Unit : Compressed Size [Total No. of Files]
** Unit : Compressed Size / Uncompressed Size [Ratio] [Total No. of Files]
Key:
Data Area
Total backup data stored in the data area
Retention Area
Total backup data stored in the retention area. Old copies of updated or deleted backup files are retained here for the number of days specified by the retention policy of the backup set before they are removed from the system.
Uploaded Size
Total data uploaded on a particular date
Total Storage
Data Area + Retention Area

Key	Description
Date	**The date that the following statistics are collected.**
Data Area	**Total number and size of backup files stored in the data area on a particular date.**
Retention Area	**Total number and size of backup files stored in the retention area on a particular date.**
Uploaded Size	**Total number and size of backup files uploaded to the backup server on a particular date.**
Total Storage	**Total number and size of backup files stored under your backup account on a particular date.**

23 Further Information

23.1 Contact Us

AGENTUR BROGLIE
Moserstr. 13
72760 Reutlingen
info@agentur-broglie.de
Tel. +49-170-3850801
www.gebro-backup.de

Appendix

Appendix A - Supported Languages

OBM supports the following languages.

Language Code	Language
bg	**Bulgarian**
ca	**Catalan**
cs	**Czech**
da	**Danish**
de	**German**
el	**Greek**
en	**English**
el	**Spanish**
eu	**Basque**
fi	**Finnish**
fr	**French**
hu	**Hungarian**
is	**Icelandic**
it	**Italian**
iw	**Hebrew**
ja	**Japanese**
ko	**Korean**
lt	**Lithuanian**
nl	**Dutch**
no	**Norwegian**
po	**Polish**

pt_BR	**Portuguese (Brazil)**
pt_PT	**Portuguese (Portugal)**
ro	**Romanian**
ru	**Russian**
sl	**Slovenian**
sv	**Swedish**
th_th	**Thai (Thai Digit)**
tr	**Turkish**
zh_CN	**Chinese (Simplified)**
zh_TW	**Chinese (Traditional)**